2006-07

Homeland Security Affairs Journal, Volume II - 2006: Issue 2, July

Monterey, California. Naval Postgraduate School

Homeland Security Affairs Journal, Volume II - 2006: Issue 2, July
http://hdl.handle.net/10945/49816

VOLUME II, ISSUE 2: JULY 2006

HOMELAND SECURITY AFFAIRS

THE JOURNAL OF THE
NAVAL POSTGRADUATE SCHOOL CENTER FOR HOMELAND DEFENSE AND SECURITY

ISSN 1558-643X HTTP://WWW.HSAJ.ORG

Changing Homeland Security: What Should Homeland Security Leaders Be Talking About?

Christopher Bellavita

Homeland security has spiraled into Stage Five of the Issue Attention Cycle.[1] Stage Five – the post-problem stage – means homeland security again operates principally behind the public apron. Stakeholders sedulously sift through the grist of homeland security's congressional, industrial, academic, and bureaucratic complex. The professionals who populate that complex spend their days calibrating the strategies, programs, and institutions disjunctively formed in the earlier stages of the Cycle.

Except for an occasional fifteen minutes of public attention to dead terrorists, disrupted plots, and grant cuts, homeland security is not an issue high on the public's agenda.[2] It could leap back on top in an instant.[3] But for now most conversations about homeland security take place within a comparatively small community.

The issues are largely the same ones talked about for the last five years: funding, threats, hazards, borders, interoperability, intelligence, response, transportation, equipment, and – recently – pandemics.[4] Unarguable progress has been made in all these domains. We clearly are better prepared – for some things – than we were in the autumn of 2001. Equally as certain, there are miles to go before most of the nation's jurisdictions get a "Sufficient" rating in future national preparedness assessments.[5]

Stage Five in the Issue Attention Cycle means there is little political will to substantially alter the hodgepodge federalism that characterizes U.S. homeland security. The system we have is the one we have to work with, at least until something significant happens: another attack, a catastrophic natural disaster, a national public health emergency, or a new political administration. [6]

Until the system is shocked, much homeland security work will be incremental. It will continue to focus on the mundane but institutionally important work of answering "how prepared are we, how prepared do we need to be, and how do we prioritize efforts to close the gap?"[7] The operational agenda will funnel attention toward measuring outputs and outcomes, and stutter fitfully around peripatetic priorities, like "creating a culture of preparedness" or modernizing "our planning processes, products, tools, and the training, education, and development of homeland security planners who are expected to use them."[8]

If the country is never attacked again, if there are no more national traumas, then incrementalism is a cautious, stable and appropriate way to continue to improve homeland security. But if something calamitous does happen, incrementalism does not stand a chance.

Ammunition and Weapons

Management attends to the realism of what is. Leadership looks toward what could be, what should be. What should the future be like in homeland security? And how can we get there?

Future-thinking homeland security leaders are like ammunition, particularly during Stage Five. They are seeking weapons – looking for opportunities to be used. Elected and other political officials are the weapons, especially primed to do battle during times of national crisis, when the Attention Cycle coils around to "alarmed discovery."

Immediately after the next national trauma, elected officials will be looking for answers, for ideas about what to do to respond to the "discovery" that we remain exposed to a cluster of vulnerabilities already familiar to homeland security specialists. Elementary schools – critical infrastructure to the parents of every student – are unprotected targets. Chemical plants – patiently waiting to be weaponized – sit in the midst of high-density populations. The medical care system has about ten percent of the ventilators needed during a pandemic. Foot and Mouth disease, caused by a virus that can easily be brought into the country, can infect livestock in an entire region and significantly affect food related businesses, employment, and economies. The list of how vulnerable the nation is to harm is practically endless.[9]

The next significant national event will create an environment that supports, if not demands, substantial change. What should those changes be? More of the same, but with added discipline and control? A rededication to the principles of authentic federalism? A re-imagining of our core civil liberties? Something completely different?

What will homeland security leaders recommend after the next tragedy? Less dramatically, what ideas will they champion when city, state, or national political administrations change?

The questions should be discussed now, before answers are needed, before emotion drowns deliberation.

Responses to these open-ended questions will emerge from conversations among people who care about homeland security when it is not on top of the nation's policy agenda. The discussions will be based on a mix of research, experience, opinion, ideology, and bias. Participants in the conversation will be political officials, interest group representatives, public administrators, academics, professional commentators, the occasional unattached citizen, and others who form the amoebic body of homeland security leaders. These are people who could be called Stage Five leaders.

You Might Be A Homeland Security Leader If . . .

Anyone who has read this far can probably name at least half a dozen people they look to for thoughtful homeland security ideas and perspectives. You can find familiar names on books and articles, in the appendices of Department of

Homeland Security (DHS) and think tank reports, and at congressional hearings.[10] Stage Five leaders routinely appear at homeland security conferences, on workshop panels, and in subject matter expert groups. Recently some of them have been featured in media tales about former government officials who moved to private industry.[11]

The leaders come from many arenas. Their ideas can help shape the future of homeland security. What should they be talking about?

"What is past is prologue" is inscribed on a statue outside of the National Archives, home of the Declaration of Independence, Constitution, and other foundational America charters.[12] The phrase implies those who are interested in the future have an obligation to know something about the past.

Homeland security is old enough to have a past. Part of that past is encapsulated in the strategies, policies, programs, and processes that shape the work of the homeland security professional. How much of this past do you know?

Try your hand at answering the following questions. Suggestively, they outline what could be called basic homeland security literacy – at least in the cognitive domain.

1. What is the official definition of Homeland Security? Absent an official definition, what is a defensible definition? How does that compare with the official definition?

2. Identify the basic elements of the nation's homeland security policy.

3. Describe the objectives of the *National Strategy for Homeland Security*. If you have a state or local perspective, also identify the objectives of your jurisdiction's homeland security strategy. Extra points if you can highlight the prevention elements in any of the strategies.

4. How many of the eight principles that shaped the *National Strategy* can you name?

5. How many homeland security presidential directives have been issued? Extra leadership points given for each one you can describe (and saying "HSPD 1, HSPD 2, …" doesn't count).

6. What is the National Preparedness Goal? What is the "vision" for the national preparedness goal? What is the difference between the two? How much of either can you recite?

7. Identify the seven priorities for national preparedness. Add extra points for being able to separate them into "overarching priorities" and "priorities to build specific capabilities." Double your point score for this question if you can repeat the rumor about an eighth priority, supposedly added after Katrina.

8. What are the National Planning Scenarios? How are they intended to help preparedness? On what basis have they been criticized? Without looking, how many can you describe?

9. What is the difference between the TCL and the UTL? How many items are in each group (plus or minus ten percent)? Where do they fit within the "culture of preparedness?"

10. Explain the difference between, and relationships among, NIMS, ICS, NRP, ESF, unity of command, and unified command. Subtract points from your final score if you have to look up the acronyms.

11. Define "risk." How is risk determined? How do you distinguish risk from threat and vulnerability? How many definitions of risk can you cite? You get one extra point for each definition, up to a maximum of 22.

12. Provide convincing distinctions among the terms prevention, protection, readiness, and preparedness. Three extra points for identifying the national policy document that defines prevention as activities undertaken "during the early stages of an incident."

13. Draw your jurisdiction's homeland security organizational or network structure. Which agency or people are the critical nodes in that system, and why? Extra points if the structure extends beyond your jurisdiction's political boundaries.

14. Explain the process used to decide the 2006 DHS grant awards. Identify how much it costs your jurisdiction – direct and indirect costs – for each dollar of homeland security funding it receives.

15. Describe how you have, or plan to, or should, measure the impact of homeland security programs and spending in your jurisdiction.

16. Have you seen and understood your jurisdiction's most recent threat assessment? If no, why not? If yes, what did you do with the information? Who do you tell what your requirements are for intelligence?

17. Have you initiated or responded to a DHS data call? Have you seen or used the results of that call? How?

18. Can you identify the most significant critical infrastructure in your jurisdiction? To whom is it significant? What proportion of your critical infrastructure is outside your ability to control or influence?

19. Describe your jurisdiction's crisis communication strategy. Additional points awarded for identifying the core message that will be communicated for specific catastrophic incidents.

20. How important is homeland security to the public officials and citizens in your jurisdiction? How do you know? Additional points if homeland security is important enough to you to have at least one emergency preparedness kit and a family crisis plan.

Extra Credit – Multiple choice (select all that apply).

You don't know the answer to some or all of the above questions, but you:

a) Know where to find the answers;

b) Know someone who can tell you the answers if and when you ever need them;

c) Know better questions to ask; or

d) Know more effective ways to figure out who the Stage Five homeland security leaders are.

What Should Stage Five Leaders Be Talking About?

How did you do? In my experience, very few homeland security leaders are able to correctly answer more than half of those somewhat pedantic questions. (In the past year, I have found only one person who can say what the vision is for the National Preparedness Goal.)

The questions have superficial face validity about one's level of homeland security literacy. However, one could argue (perhaps convincingly) that knowing details is not what leadership ought to be about. Leadership should be about big-picture issues; the forest rather than the trees; the 30,000-foot view of homeland security – pick your own metaphor. Details – although important – are for the people who manage what leaders create.[13]

Three Big Homeland Security Pictures

There are at least three big-picture perspectives that can frame conversations about the future of homeland security: strict constructionism, middle-of-the-road moderation, and radical reconstructionism.[14]

The traditional view – if one can use the word "traditional" with anything related to homeland security – is that homeland security initially was about preventing and responding to terrorism.[15] The post-Katrina and the pre-pandemic political environment has expanded the scope of what constitutes homeland security. Should that expansion be resisted, embraced, ignored?

Strict constructionists embrace the traditional perspective. They maintain homeland security is about terrorism, pure and simple, just as it says in the *National Strategy*. Other agencies deal with other policy issues. Homeland Security can collaborate with them. Let FEMA, state, and local emergency management agencies have natural disasters. Public health can take the lead for pandemics. The terrorism portfolio belongs unambiguously to homeland security.

Middle-of-the-road moderates are in a second group. They agree homeland security is about terrorism. But they say it should and could be about more than that. Concentrating too much on terrorism reduces overall readiness. They offer the Katrina response as evidence.

"9/11 was a distraction for us," said one western state emergency management official. "Our threats are wildfires and tornados. Since homeland security showed up, we've gotten away from planning, training and doing exercises about our actual threats. Now people are too busy writing homeland security grants and reports to work on our real issues. If anything, we've fallen behind."[16]

"When are we going to be finished with this preparedness business so we can get back to our regular work?" asked an eastern state administrator.[17]

Middle-of-the-road moderates draw attention to the dual-use value of emergency preparedness structures and processes.

One state emergency management leader said, in response to criticisms that terrorism displaces effort, "What we do to get prepared for an all hazards response can help us respond to other threats, like terrorism and pandemics." [18]

Radical reconstructionists advocate a third perspective. They assert that homeland security is about much more than stopping the next terrorist attack, responding to natural disasters, or getting ready for pandemics. The public safety disciplines struggling to find unifying themes can help the nation by paying more attention to the social and economic conditions that give rise to and support "premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents, usually intended to influence an audience."[19]

A lexicographer cautions not to "confuse *sécurité*, the feeling of having nothing to fear, and *sûreté,* the state of having nothing to fear."[20] Radical reconstructionists focus on the state of having nothing (or at least less) to fear. They contrast the comparatively few Americans who have been killed by terrorists with the substantial number of people killed each year by traffic accidents, tobacco, seasonal flu, and other preventable events. They ask why homeland security is not more concerned with gang violence, illegal drugs, inadequate public health and medical care, second-rate educational systems, and

other domestic policy problems that ultimately have as much to do with homeland *sûrete* as countering terrorism.[21]

Many of our national homeland security and defense-related strategies have short-term and long-term elements.[22] Short-term strategic work is directed at immediate problems. Long-term activities aim to address underlying causes of those problems.[23] Self-starter Islamic fundamentalist terrorists are a growing domestic threat.[24] Left and right wing domestic terrorists are still active.[25] Homeland security needs both short- and long-term perspectives. From a social perspective, its current operational point of view is too short, too narrow.

Radical reconstructionists argue the behemoth that is the Department of Homeland Security – and eventually its state and local functional counterparts – could usefully collaborate with other agencies to dampen the social conditions that contribute to domestic unrest, including terrorism. How many years without attacks have to pass before politicians stop providing forty billion dollar budgets? How many uninsured or underemployed or uneducated does it take to create a homeland security problem? As those who focus on social capital and the community development dimensions of homeland security suggest, "It's tough to be a terrorist in a caring community."[26]

AN INVITATION

The conversational terrain shaping the future of homeland security sits somewhere between being able to recite the National Preparedness Goal and advocating that DHS evolve into a social services agency.

Regardless of how you did on the basic literacy test, or what big picture you may subscribe to, you are invited to participate in a thought experiment to answer the question: What should homeland security leaders be talking about?

Envision a strategic conversation among Stage Five leaders. The conversation is strategic in the sense that it concentrates on the large purposes and activities of homeland security as a policy area within the wider social, economic, and political environment.[27] It is oriented more toward the possibilities of the future than the pressing concerns of today. It is a conversation in the sense of civil communication among participants. It is characterized by cognitive and affective maturity, listening, risking, and learning. That is the premise for the experiment. Now, what are the participants in this conversation talking about?

If you are interested in sharing your thoughts, please send an email to cbellavi@nps.edu describing what you think Stage Five homeland security leaders ought to be talking about and why.

We will publish creative, provocative, and thoughtful responses in the next issue of *Homeland Security Affairs*.

[1] Christopher Bellavita, "The Issue Attention Cycle," *Homeland Security Affairs* 1, no. 1 (2005). "... Anthony Downs ... argued that certain issues follow a predictable five stage process: pre-problem, alarmed discovery, awareness of the costs of making significant progress, gradual decline of intense public interest, and the post problem stage. Before the [July 2005] London attacks, homeland security was on the cusp of Stage Five. After the attacks, it revisited Stage Two. Before too many months pass, it is likely to recall the difficulties of Stage Three, make a brief return trip through Stage Four, and – if there are no more attacks – settle into Stage Five."

[2] Polling data present a mixed picture on this point. When people are asked about the important problems facing the country, terrorism is rarely mentioned by more than ten percent (See *ABC News/Washington Post Poll*, June 22-25, 2006; *CBS News Poll*, May 16-17, 2006; *The Harris Poll*, May 5-8, 2006; *FOX News/Opinion Dynamics Poll*, May 2-3, 2006; and *NBC News/Wall Street Journal Poll*, April 21-24, 2006.). Other polls, however, suggest protecting the nation against further terrorist attacks should be an important priority for Congress and the executive branch (see *CNN Poll*, May 16-17, 2006; *Gallup Poll*, March 13-16, 2006; and Pew Research Center survey, Jan. 4-8, 2006). If homeland security were important to Americans, one would expect to see that importance reflected in behavior. An October 2005 survey (one month after Katrina) found that "Americans are no more prepared for a natural disaster or terrorist attack [in 2005] than they were in 2003." There was "a significant decline in both those who indicate that they have a disaster plan and those who indicate that they have an emergency supply kit." (*Citizen Preparedness Review*, "A Quarterly Review of Citizen Preparedness Surveys," February 2006: http://www.orcmacro.com/ORCMacroPreparednessSurvey.pdf.). The "Terrorism Index," published by *Foreign Policy* (July/August 2006) shows a wide gap between the perceptions of foreign policy experts and the American public about terrorism-related issues. The Index data adds support to the hypothesis advanced in this article about core, or Stage Five, leaders.

[3] Polls show people express more concern about terrorism and homeland security in the immediate wake of incidents like the Madrid or London bombings. See, for example, *CNN/USA Today/Gallup Poll*, July 12, 2005. Jenkin, following Slovic, discuses this phenomenon as the "signal value" of an event. See Clinton M. Jenkin, "Risk Perception and Terrorism: Applying the Psychometric Paradigm," *Homeland Security Affairs* 2, no. 2 (July 2006). (It will be interesting to see if the July 11, 2006 bombing in Mumbai has any signal value for a Euro-centric U.S. citizenry.) In addition, there is a perspective that says the Republican party fares better with the public than the Democratic party on terrorism issues (for an example, see the historical data provided by the *ABC News/Washington Post Poll*, June 22-25, 2006). If this perception is correct, one would expect to see terrorism and homeland security issues become more important as the 2006 congressional election season approaches. For a theoretical perspective on this issue, see Nick Pidgeon, ed., *The Social Amplification of Risk* (Cambridge University Press, 2003).

[4] "National Survey of State Homeland Security Leaders," (Western Carolina University, Institute for the Economy and the Future, 2006); Center for Best Practices, "2006 State Homeland Security Directors Survey," (National Governors Association, 2006).

[5] Department of Homeland Security, "Nationwide Plan Review: Phase 2 Report," (2006), 4.

[6] The emphasis on working with what exists rather than creating new approaches was illustrated by George Foresman, DHS Undersecretary for Preparedness, during a January, 24, 2006 conference presentation. Foresman said, "We have been overly focused on the products we produce. We have missed the process. We need progress, not perfection."

[7] "Department Of Homeland Security Releases Interim National Preparedness Goal," April 1, 2005, http://www.dhs.gov/dhspublic/display?content=4420; accessed June 21, 2006.

[8] United States Government, "The Federal Response to Hurricane Katrina: Lessons Learned," (February, 2006), 79 ff; Department of Homeland Security, "Nationwide Plan Review: Phase 2 Report," xii.

[9] Katherine Hobson, "Are We Ready?" *U.S. News and World Report*, May 1 2006; John Cline, "State and Local Policy Considerations for Implementing the National Response Plan" (Naval Postgraduate School, 2005 March); Richard Clarke, et al. *The Forgotten Homeland* (Century Foundation, 2006); Center for Best Practices, "National Survey of State Homeland Security Leaders," *2006 State Homeland Security Directors Survey*; Michael E. O'Hanlon, et al., *Protecting the Homeland* (Brookings Institution Press, 2006). On unconventional weapons of mass destruction see Boyd Bender, "Sept. 11 – One Year Later I: Weapons of Mass Destruction Are Top Threat," *Global Security News*, 2002 [cited June 21 2006], available at http://www.globalsecurity.org/org/news/2002/020909-wmd.htm. For information about Bruce Schneier's "Big Book of Terrorist Plots" (based on an internet contest to identify "unlikely, yet still plausible, terrorist attack scenarios"), see "The Scariest Terror Threat of All," *Wired News*, June 15, 2006, available at http://www.wired.com/news/columns/0,71152-0.html?tw=wn_story_page_prev2.

[10] See, for examples, O'Hanlon, *Protecting the Homeland*; Clarke, *The Forgotten Homeland*; and Department of Homeland Security, "Nationwide Plan Review: Phase 2 Report," Appendix E. See also articles and links at http://www.heritage.org/Research/HomelandDefense/index.cfm, http://www.sourcewatch.org/index.php?title=Homeland_security, and http://www.comw.org/tct/homeland.html#1.

[11] Eric Lipton, "Former Antiterror Officials Find Industry Pays Better," *New York Times*, June 18 2006.

[12] The phrase is from Shakespeare's *The Tempest* (Act II, Scene 1). The statue, called "The Future," is by Robert Aitken. Interestingly, or perhaps disturbingly, "The Future" rests outside an entrance to the National Archives that is no longer used. The picture is from http://www.fhwa.dot.gov/infrastructure/pa14.htm.

[13] On the other hand, maybe leaders should know details. Philip Evans and Bob Wolf suggest that in what they call "vibrant human networks…the credibility and…authority of leaders derives from their proficiency as practitioners. The content of leaders'…communication is less *about* work than it *is* work." [Emphasis in the original.] From "Collaboration Rules," *Harvard Business Review* (July-August 2005), 101.

[14] These three perspectives are presented in the Weberian, "ideal type" sense. H.H. Gerth and C. Wright Mills, *From Max Weber* (New York: Oxford University Press, 1946), 59. See also Lewis A. Coser, *Masters of Sociological Thought: Ideas in Historical and Social Context*," second edition (New York: Harcourt Brace, 1977), 223-224. "An ideal type is formed by the one-sided accentuation of one or more points of view and by the synthesis of a great many diffuse, discrete, more or less present and occasionally absent concrete individual phenomena, which are arranged according to those one-sidedly emphasized viewpoints into a unified analytical construct." One reviewer of this article suggests there may be at least two more perspectives. One view suggests "preparing for terrorism prepares everyone for everything else, rather than vice-versa. Seems like a little thing unless you are in charge of funding and resources. In that case the "flavor" of execution can be vastly different." Another perspective sees homeland security as the "catch-all for all we do in the realms of public safety, public health and public security. It's not terrorism vs. natural event focus; it is EVERYTHING. I think this is where some in current DHS think they are."

[15] Department of Homeland Security, *National Strategy for Homeland Security* (2002).

[16] Comment from a state emergency management audience member at a May 2006 homeland security conference.

[17] Reported by a state preparedness officer during a June 2006 pandemic flu conference

[18] Comment by a National Emergency Management Association executive in an off-the-record meeting, May 2006. The middle-of-the-road moderate's perspective is also reflected in "The Federal Response to Hurricane Katrina: Lessons Learned," (page 68): "We have thought of terrorism and natural disasters as competing priorities rather than two elements of a larger homeland security challenge."

[19] Title 22 of the US Code, Section 2656f(d).

[20] Marguerite-Marie Dubois, *Larousse Modern Dictionary* (Paris: Libarie Larousse, 1960), 657. Cited in David Jablonsky, "The State of the National Security State," *Parameters* (Winter 2002-03), 4-20. While the comment was about semantics, there are functional implications for the work of homeland security. For an extended discussion on the affective elements of risk, see Jenkin, "Risk Perception and Terrorism."

[21] DHS elements are already involved in counter-gang and counter-narcotic interventions, pornography, medical care and other activities not typically associated with terrorism. See the illustrative documents at http://www.dhs.gov/dhspublic/theme_home1.jsp.

[22] For examples, see the *National Strategy for Combating Terrorism,* http://www.hsdl.org/homesec/docs/whitehouse/counter_terrorism_strategy.pdf, *National Security Strategy of the United States of America,* http://www.hsdl.org/homesec/docs/whitehouse/nps08-031606-01.pdf, and the *National Strategy for Homeland Security,* http://www.hsdl.org/homesec/docs/whitehouse/nat_strat_hls.pdf.

[23] Daniel Benjamin and Steven Simon, *The Age of Sacred Terror* (New York: Random House, 2002), Chapter 11.

[24] Daniel Benjamin and Steven Simon, *The Next Attack: The Failure of the War on Terror and a Strategy for Getting It Right* (New York: Henry Holt and Company, 2005), 27-31. Scott Shane et al. "F.B.I. Killed Plot in Talking Stage, A Top Aide Says," New York Times, June 24, 2006, http://select.nytimes.com/search/restricted/article?res=F20F1EFB3D540C778EDDAF0894DE404482. Ian Austen and David Johnston, "17 Held In Plot To Bomb Sites Across Ontario," *New York Times*, June 4, 2006, http://select.nytimes.com/search/restricted/article?res=FA0710F73C550C778CDDAF0894DE404482.

[25] For a review, see Timothy G. Baysinger, "Right-Wing Group Characteristics and Ideology," *Homeland Security Affairs* 2, no. 2 (July 2006) http://www.hsaj.org.

[26] Phil Palin, *Preparing for Catastrophe: Prevention and the Role of Law Enforcement* (New York: McGraw Hill, 2006). For the social capital argument, see Russell R. Dynes, "Social Capital: Dealing with Community Emergencies," *Homeland Security Affairs* 2, no. 2 (July 2006). For a discussion about other foci for homeland security, see Marc H. Morial, "Homeland Security Overshadow Efforts to Keep Rates Down," *Louisiana Weekly,* July 10, 2006 (available online at http://www.louisianaweekly.com/weekly/news/articlegate.pl?20060710v). For an argument that the nation should expand its counter-terrorism tools, see Don Reed, "On Killing Al-Zarqawi - Does United States Policy Know Its Tools in the War on Terror?" *Homeland Security Affairs* 2, no. 2 (July 2006): "Effective application of the information tool is prescribed within the National Strategy for Homeland Security, but it does not mention the use of the political, economic, or social tools for domestic counterterrorism."

[27] Peter Vaill, *Managing as a Performing Art* (San Francisco: Jossey-Bass, 1989), 162.

On Killing al-Zarqawi – Does United States Policy Know Its Tools in the War on Terror?

Donald J. Reed

> *"Do not rejoice that you killed (al-Zarqawi), he has left behind lions that ... trained under him."*
> Statement attributed to al-Zarqawi's reported successor Abu Hamza al-Muhajir.[1]

TERRORISM PROCESSES VERSUS TERRORIST ENTITIES

The air attack that killed al Qaeda leader Abu Musab al-Zarqawi – the successful synchronization of actionable intelligence and tactical military operations that eliminated a key terrorist network node – was a good thing. Much of the media-pundit and popular analysis that followed has focused on the potential impact of al-Zarqawi's death on the outcome of the war in Iraq. The demand of the American public for information and results notwithstanding, the emphasis on outcome is not the right approach. Al-Zarqawi's death serves greater strategic purpose both in the war in Iraq, and in the larger war on terror, when viewed as process rather than as outcome or end-state.

The diffusion of threat specificity when viewing terrorism as a methodology, exemplified by the terror network known as al Qaeda, makes strategic thought difficult. Conventional wartime strategy has traditionally concerned itself with identifying enemy weaknesses or centers of gravity and using military force to strike at them. The issue becomes how to craft a strategy to exploit an asymmetrical enemy's weaknesses without always knowing who the enemy is, or even what means of war he will employ. A war that encompasses literally any group using terrorist tactics becomes impossibly broad, engulfing a wide range of groups that includes those posing no meaningful threat to the United States.

In the war on terror it becomes necessary therefore to distinguish between terrorism as a process and terrorist networks as entities. Terrorism, as a process, includes sub-processes that can be disrupted through the networking of political information security (i.e. military or law enforcement), economic, and social means. Those sub-processes vulnerable to disruption include: leadership development; alliance building; public and ideological outreach; acquisition of funding, materiel, shelter and support; recruitment; organization of efforts; indoctrination and training of personnel; planning and targeting; movement and operations; communications; and exploitation of results.[2] When viewed as entities, different targeted strategies are required to defeat individual terrorist networks depending on whether their ideologies are rooted in political, economic, cultural, or special-interest origins. Strategies focused against specific terrorist networks can be resource-intensive and there is no guarantee of success. It is not likely that terrorism can be eliminated by targeting terrorist networks, but by disrupting their processes terrorist networks can be contained or rolled back.

While it constitutes a tactical success and a great moral victory for the United States, it is likely that the death of al-Zarqawi will have little effect on either al Qaeda or the ongoing insurgency in Iraq. With a structure that has been described as "horizontal as opposed to hierarchical, and ad hoc as opposed to unified" the Iraqi insurgency has achieved the resiliency of a network.[3] Removal of key nodes in the network leaves the remaining key nodes and links, and the white space between them intact and functioning. According to Bruce Hoffman of the RAND Corporation, "There is no center of gravity, no leadership, no hierarchy [to the Iraqi insurgency]; they are more a constellation than an organization. They have adopted a structure that assures their longevity."[4]

If al-Zarqawi's death leaves the Iraqi insurgency and al Qaeda intact and capable of continuing to fight, the questions for the United States become: Does his death advance United States policy in the war in Iraq, and the overall war on terror? How successful is the United States in disrupting the processes of the Iraqi Insurgency and of al Qaeda? As a corollary, what are the domestic implications? The answer perhaps can be found in the tools of policy that are available to the United States although its track record in using them has not always been good.

UNITED STATES POLICY AND ITS TOOLS IN IRAQ

In *On War*, in his discussion of war as an instrument of policy and the relationship between political and military interests, Carl von Clausewitz speaks of the "assumption that policy knows the instrument it means to use."[5] United States policy for Iraq, as established by the *National Strategy for Victory in Iraq* is a nation that is "peaceful, united, stable, *democratic* and secure [italics added]."[6] The tools by which the United States means to achieve its policy, as laid out in the *Strategy*, are political, security (i.e. military) and economic. Noticeably missing from the *Strategy* are effective applications of the information tool, which includes strategic communications, and the social tool, which includes culture and religion.

If we accept Clausewitz's supposition as true, then it is not self-evident that United States policy knows the instrument it means to use in Iraq, despite the occasional military success in removing terrorist nodes such as al-Zarqawi. It appears the United States has elected to use military means as its primary tool to establish the necessary political, security and economic pre-conditions and processes for democracy in Iraq. It does not seem to focus at all on the social pre-conditions for democracy. This is a problematic approach.

Much of United States' effort in Iraq from 2003-2005 has relied heavily on military occupation and counter-insurgency efforts to establish democratic processes. Thus far, they have produced very mixed results and it is not certain the means being used – military – are the correct means at all. Anthony Cordesman, of the Center for Strategic and International Studies, has touched upon this issue. In *Rethinking the Challenge of Counterinsurgency Warfare: Working Notes*, he writes, "Democracy is the last, not the first, priority [when fighting an insurgency]. Security, effective governance and services, rule of law and limits to corruption, education, health, and employment all have a much higher priority." [7] It is here, in the processes for achieving the priorities laid out

by Cordesman, that the death of al-Zarqawi has the potential to serve its greatest purpose.

The proof of this assertion is in the lack of progressive results thus far. From 2004-2005 the nature of the insurgency in Iraq – an insurgency the Bush Administration was reluctant to recognize – changed. During this period the number of American troop deaths in Iraq declined by six percent and the number of American troops wounded declined by thirty-three percent. This is not, however, an indicator of progress in achieving the stated goal of a democratic Iraq. As reported by the Center for Strategic and International Studies, at the same time American casualties were declining the Iraqi populace experienced a different and much starker reality: an increase in insurgent attacks and in casualties, as shown in the table below.

The Nature of Attacks in Iraq, 2004-2005

NATURE OF ATTACKS	2004	2005	Difference
Insurgent Attacks	26,496	34,131	+ 29%
U.S. Troops Killed	714	673	- 6%
U.S. Troops Wounded	7,990	5,369	- 33%
Car Bombs	420	873	+ 108%
Suicide Car Bombs	133	411	+ 209%
Suicide Vest Attacks	7	67	+ 857%
IED Attacks	5,607	10,953	+ 95%

Notes:
1. The average success rate (attacks that cause damage or casualties) = 24%
2. Insurgent attacks focused more on Iraqis and less on U.S. forces in 2005.
3. The total number of U.S. casualties dropped from 2004 to 2005 but the number of attacks increased.

Reliable figures are difficult to obtain but the Center for Strategic and International Studies indicates that, by one media estimate, for every United States soldier killed in Iraq at least thirteen Iraqi civilians are killed. Its conclusion is that the trends indicate "cycles in an evolving struggle, but not signs that the struggle is being lost or won…There have, as yet, been [no] decisive trends or no tipping points: simply surges and declines."[8] The increase in Iraqi casualties reflects a shift in the focus of the al-Zarqawi-led insurgency away from attacking United States and Coalition forces and toward igniting a sectarian civil war between Sunni and Shiite Muslims. These conditions hardly seem conducive to convincing the Iraqi people that democracy is working for them.

The United States' Track Record in Fostering Democracy

If the military and security conditions for achieving democracy in Iraq remain uncertain, the political, economic, and social conditions are even more so. In a 2003 article entitled "Democracy? In Iraq?," Chappell Lawson and Strom Thacker of the Hoover Institution on War, Revolution and Peace at Stanford University, concluded that while United States efforts are not completely hopeless, "Iraq is unlikely to sustain democratic institutions, even given protracted U.S. occupation." They base their conclusion on empirical studies that indicate "Iraq has few of the success factors associated with democracy, such as a high degree of economic development and a Western cultural tradition."[9]

Lawson and Thacker measured levels of democracy on a numerical scale during 1996-2000. Not surprisingly, Iraq under Saddam Hussein scored lowest on the scale along with other countries such as Afghanistan (under the Taliban), Burma, Cuba, Libya, North Korea, Saudi Arabia, Somalia, Sudan, Turkmenistan, and Vietnam. From their data they concluded that richer, more literate, more egalitarian, and more homogenous societies do better at establishing and sustaining democracy. Petro-states, countries with high Muslim populations, and societies with little cultural affinity for the West tend to be less democratic. Lawson and Thacker conclude that Iraq would likely not become a free society on its own.

Lawson and Thacker also looked at the impact of American occupation on the likelihood of a country establishing and sustaining democracy. In the last century the United States has occupied nineteen countries with the goal of reshaping their political systems. They found that in about half the cases democratic institutions lasted, but in the other half they did not. At best, American occupation seems to be only a modest and indirect influence on the future long-term development of other countries. Those countries that became democratic following American occupation already had the necessary social, economic, and political pre-conditions that made them more likely to do so, and those that did not have those indicators were unlikely to make the transition.

Domestic Implications

As the terrorist attacks of 9/11 demonstrated, no longer can the United States rely on the conventional protections of time and distance as a result of being surrounded by vast oceans and air space. Instead, unconventional attacks may

come with little or no warning, and they may occur against United States citizens and interests at home as well as abroad. In the war on terror future attacks on the United States may originate from within as well as from outside the nation's borders. The question of whether policy knows its tools is equally applicable on the domestic front.

United States policy for domestic counterterrorism is established by the *National Strategy for Homeland Security*, which calls for preventing terrorist attacks within the United States, reducing America's vulnerability to terrorism, and minimizing the damage from attacks that do occur.[10] Unlike the war in Iraq where the primary United States policy tool is military, the primary policy tool for domestic counterterrorism is law enforcement. The National Vision for domestic counterterrorism established by the *National Strategy for Homeland Security* is to "redefine our law enforcement mission to focus on the prevention of all terrorist acts within the United States, whether international or domestic in origin."[11] Effective application of the information tool is prescribed within the *National Strategy for Homeland Security*, but it does not mention the use of the political, economic, or social tools for domestic counterterrorism.

Similar to the insurgency in Iraq the greatest domestic terrorist threat comes from resilient terror networks, whether transnational or domestic. Realizing that not all potential threats can be prevented, a network-centric response that incorporates all the tools of policy – political, information, security (military or law enforcement), economic and social – is required. Network-centric operations refers to the linking of people and systems into a common shared awareness network at all levels – international, federal, state, local, tribal, private – to obtain information superiority and enhanced decision-making and response. The working theory of network-centric operations is that organizations and agencies that are networked will outperform organizations and agencies that are not networked. Within such a concept, the transit of threats from their source to their targets at the local level presents a series of processes that can be disrupted in order to defeat, deter, preempt, prevent, protect and respond to them.

The concept of network-centric operations, however, is not simply about technology, *per se*; it is also about behavior. The idea is to feed information as quickly as possible to leaders and operators so they can make better-informed decisions about what, when and how to respond to threats. In contrast to traditional operations that are agency-specific, network-centric operations focus on passing information and intelligence among different agencies and entities to increase their ability as a whole to respond to threats.

THE WAY AHEAD

If United States policy is to be successful in the war on terror, if democratic processes are to have a chance to take root in Iraq and if terrorist attacks within the United States are to be prevented, it will be necessary for United States policy makers to adhere to Clausewitz's assumption that "policy knows the instrument it means to use." In doing so, they must use all the tools available – diplomatic, information, military/law enforcement, economic and social – to disrupt the processes of terrorism while simultaneously fostering the processes by which democracy can flourish. Of these tools, the security – military and law

enforcement – option offers the lowest probability of long-term success, particularly if wielded in isolation from the other tools. Unless the processes that breed them are addressed there will always be another al-Zarqawi to confront.

Unfortunately, there are signs that the administration does not understand Clausewitz's assumption, as it is scaling back funding for the main organizations trying to build democratic institutions in Iraq such as political parties and civil society groups. According to the *Washington Post*, agencies such as the National Democratic Institute for International Affairs and the International Republican Institute will see their grants from the U.S. Agency for International Development dry up in 2006, leaving them only special funds earmarked by Congress last year. Similarly, the U.S. Institute of Peace has had its funding for Iraq democracy promotion cut by sixty percent, and the National Endowment for Democracy expects to run out of money for Iraqi programs by September 2006.[12]

Writing in the *New York Times*, Retired Marine Corps Colonel Thomas X. Hammes, author of *The Sling and the Stone: On Warfare in the 21st Century*, outlines what he calls a laundry list of United States inaction in Iraq.[13] Among the actions that Hammes says greatly increase the likelihood of civil war are diversion of nearly half the money allocated to reconstruction in Iraq to other needs, including security; cuts in financing for democratization efforts, many of them undertaken by nongovernmental groups; proposals for cutting overall Army and Marine forces for fighting the "long war" in Iraq; inauguration of only four of the proposed sixteen Provincial Reconstruction Teams; and continuous undermanning of Army staffs and units in Iraq, even those training Iraqi security forces. The result, according to Hammes, is,

> The [Iraqi] militias are already looking ahead: some are carving out safe areas they will use as bases in the coming [civil] war by driving Iraqis of other ethnic and religious groups out of mixed neighborhoods and villages. Iraqi government officials estimated that more than 100,000 families have already fled their homes. This falling back on militias and preparing for internecine conflict is not a new phenomenon. It is exactly what we saw in Afghanistan nearly two decades ago. Once the Afghans believed the Soviet troops were finally pulling out, the various insurgent groups stopped fighting the invaders and began positioning for a multisided civil war. That conflict, of course, lasted until the United States invaded Afghanistan in 2001.[14]

On the domestic front, the United States faces the risk of complacency in the war on terror and much more needs to be done to build networks for confronting the terrorist threat. Nearly five years after the attacks of 9/11 and the pronouncement of a Global War on Terror, metrics for performance related to clear and obtainable national objectives are largely lacking. Measurements are inextricably linked to strategies. While the goals of terrorist groups may be diametrically opposed to those of the United States, however, they may also be tangential in nature with each side achieving objectives and making progress according to their different measurement systems.

It remains an open question as to why al Qaeda has not followed its attacks of 9/11 with additional attacks on the United States. The absence of attacks could be taken as an indicator of successful Homeland Security countermeasures implemented by the United States. Another alternative could be that the 9/11 attacks allowed al Qaeda to accomplish its strategic objectives and it sees no need for further attacks on the United States at this time. Uncertainty with respect to wartime strategies and measurements makes it difficult to determine or to demonstrate progress.[15]

Writing nearly four years after the 9/11 attacks, John Arquilla, co-editor of *Networks and Netwars: The Future of Terror, Crime, and Militancy*,[16] describes the way ahead on building counterterrorism networks:

> If we … see ourselves as just part of a network fighting for civil society worldwide, good things are going to happen. And good things will keep happening as long as our police, military and intelligence agencies come to realize that their strength grows from networked information-sharing with each other. This is a lesson not yet learned at the top, despite the examples provided by real successes of networking achieved by our allies. Failure to learn this lesson would leave us ill prepared to defend the U.S. against either Al Qaeda or other networks likely to rise in the coming years, in emulation of Bin Laden, the dark pioneer of netwar.[17]

Given the current outlook, until the United States begins to use effectively all its tools of policy both in Iraq and on the domestic front, and focuses on processes rather than tactical outcomes, the conclusion to be drawn is that there will be an endless line of al-Zarqawi, or even Bin Laden, successors and the future will remain uncertain. The terrorist threat will remain unabated and the lessons learned, or not learned, will carry over to the larger war on terror overall.

Donald (Don) J. Reed *is the Defense Support of Civil Authorities Officer, J35 Future Operations, U.S. Northern Command in Colorado Springs, Colorado. He specializes in strategic-level homeland defense and homeland security planning throughout the continental United States, Alaska, Puerto Rico, and the U.S. Virgin Islands. His career spans twenty years as a U.S. Army military police officer, and more than four years as a civilian homeland defense plans supervisor. He helped to plan the Department of Defense operational response to the 9/11 terrorist attacks, and the later response to Hurricane Katrina as a member of Joint Task Force Katrina. Mr. Reed holds a bachelor degree in Forensic Studies from Indiana University; a master's degree in Administration of Justice from Webster University; and a master's degree in Security Studies from the Naval Postgraduate School, where he is also a recipient of the Curtis H. "Butch" Straub Award from the Center for Homeland Defense and Security.*

[1] Aljazeera.net, "Zarqawi Successor Vows Vengeance," June 13, 2006. http://english.aljazeera.net/NR/exeres/988B0002-1C7E-43B7-8DAE-6206474EF106.htm.

[2] *Combating Terrorism: The Challenge of Measuring Effectiveness,* Congressional Research Service Report for Congress, Order Code RL33160, Library of Congress, November 23, 2005, 5.

[3] *New York Times*, "Profusion of Rebel Groups Helps Them Survive In Iraq," December 2, 2005, 1.

[4] Ibid.

[5] Carl von Clausewitz, *On War,* Edited and translated by Michael Howard and Peter Paret (Princeton, New Jersey: Princeton University Press, 1976), 607.

[6] *National Strategy for Victory in Iraq* (Washington, D.C.: Government Printing Office, 2005), 3. http://www.whitehouse.gov/infocus/iraq/iraq_national_strategy_20051130.pdf .

[7] Anthony Cordesman, *Rethinking the Challenge of Counterinsurgency Warfare: Working Notes* (Washington, D.C.: Center for Strategic and International Studies, November 7, 2005).

[8] *Iraq's Evolving Insurgency: The Nature of Attacks and Patterns and Cycles in the Conflict,* Working Draft, Revised (Washington, D.C.: Center for Strategic and International Studies, Washington, D.C., February 2, 2006).

[9] Chappell Lawson and Strom C. Thacker, "Democracy? In *Iraq*?" *Hoover Digest* 3 (Summer 2003).

[10] *National Strategy for Homeland Security* (Washington, D.C.: U.S. Government Printing Office, 2002), 2.

[11] Ibid, 26.

[12] *Washington Post*, "Democracy in Iraq Not a Priority in U.S. Budget," April 5, 2006.

[13] Thomas X. Hammes, Colonel, USMC, *The Sling and the Stone* (St. Paul, Minnesota: Zenith Press, 2004); Thomas X. Hammes, "Tearing Iraq Apart," *New York Times*, June 1, 2006.

[14] Ibid.

[15] *Combating Terrorism*, 2.

[16] John Arquilla and David Ronfeldt (editors), *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Santa Monica, CA: RAND Corporation, 2001).

[17] John Arquilla, "It Takes A Network," *Los Angeles Times (*August 25, 2002).

Right-Wing Group Characteristics and Ideology

Timothy G. Baysinger

INTRODUCTION

Following the September 11, 2001 World Trade Center attack, our national attention was focused on Osama bin Laden, al Qaeda, and other radical Islamic extremists. On April 19, 1995 the Alfred P. Murrah Federal Building was bombed by a native-born white male United States citizen who harbored right-wing extremist beliefs. While our collective consciousness prioritizes radical Islamists as the preeminent threat, should individuals and groups that encompass the radical right be viewed as having a reduced capacity to perform acts of terrorism? What future trends will be adopted by the radical right? How could these trends lead to an escalation of the threat posed by right-wing extremists? What can be done to reduce the threat of terrorism perpetrated by right-wing adherents? Before offering an answer to these questions, we should establish a knowledge baseline to understand the history, key figures, and beliefs of right-wing extremist groups in the United States.

The specific ideology of right-wing extremism is frequently difficult to define because adherents have multiple and frequently simultaneous memberships in the array of right-wing groups. Many people involved in right-wing groups have come from other right-wing organizations and will likely move on to other groups as their beliefs change.[1]

CHRISTIAN IDENTITY MOVEMENT

To understand Christian Identity is to understand a core feature of right-wing extremism. While some right-wing groups and individuals do not embrace the ideas of the Christian Identity movement,[2] it has become a prominent religious belief for many right-wing extremists.

Theology

According to David Brannan in "Left- and Right-wing Political Terrorism," a chapter in *The Politics of Terrorism,* Christian Identity is comprised of two separate theological ideas. The first and most prevalent form of Christian Identity is referred to as "seed-line" theology. In "seed-line" theology, Jews are depicted as the actual offspring of the Devil (Lucifer) and Eve. All non-whites, according to 'seed-line' theology, are considered to be the "beasts in the field," a reference to the biblical passage contained in Genesis 1:24. Right-wing extremists who embrace "seed-line" Christian Identity theology possess core beliefs to justify death, enslavement, or expulsion of all non-whites from the country.[3]

The British-Israel version of Christian Identity is the second theological belief embraced by right-wing extremists. According to Brannan, British-Israel followers believe Aryans, rather than the Jews, are God's chosen people. True Israel is actually comprised of the Anglo-Saxon, British, Scandinavian, and

Germanic peoples, not Semitic or Ashkenazi Jews.[4] Pete Peters, the pastor of the LaPorte Church of Christ in Colorado preaches British-Israel Christian Identity theology. Part of Peters' message is that Jews are not God's chosen people and true Israelites are the Celtic, Anglo Saxon, Scandinavian, Germanic, and kindred people. Peters claims these true Israelites "can be identified Biblically, historically, and archeologically."[5] Bertrand Comparet, an earlier figure associated with the formative years of Christian Identity, in his essay *Christian Identity: What is It?* provides an account of Adam's people. Comparet notes the name Adam, in Hebrew, refers to being able to "show blood in the face; to be fair; rosy cheeked; to be ruddy; and to be able to blush or flush."[6] This description fits the true Israelites of British-Israel theology.

Both "seed-line" and British-Israel Christian Identity adherents refer to information contained in *The Thirteenth Tribe* by Arthur Koestler to support their views of modern day Jews. Koestler claims the majority of Jews surviving the holocaust were of eastern European descent, primarily the Khazar Empire.[7] The Khazar Empire was a Jewish state comprised mostly of Turks, prominent between the seventh and tenth centuries. It was located in eastern Europe and controlled a vital area between the Caspian Sea and the Black Sea.[8] After the destruction of their empire, Khazar tribes and communities were believed to have migrated to Russia and Poland, where the largest populations of Jews were located during the beginning of the Modern Age. According to Koestler, this migration has led many historians to speculate that a majority of the Jews in the world today may not be of Semitic origin; they may actually be of Khazar ancestry.[9]

Christian Identity History

During the middle part of the nineteenth century, the idea of British-Israelism became a movement as a result of the works of John Wilson. His book, *Lectures of Our Israelitish Origin*, his speeches, and other writings appealed to the British middle class.[10]

According to James Aho in *The Politics of Righteousness: Idaho Christian Patriotism*, British-Israelism was imported to Canada and then passed on to the United States through two points of entry. First, in 1928, Howard Rand of Maine started spreading the British-Israel message through his newsletter, the *Kingdom Message*. In 1930, Rand met William J. Cameron, the editor of Henry Ford's *Dearborn Independent*, and eventually they formed the Anglo-Saxon Federation of America.[11] The *Dearborn Independent* was a very anti-Jewish publication and was later used as the basis of Henry Ford's book *The International Jew: The World's Foremost Problem*.[12]

The other location for the export of the British-Israel movement to the United States was Vancouver, British Columbia, which influenced followers in Washington and Oregon. A British-Israel group in Vancouver influenced the emergence of Christian Identity through its participation in a series of conferences held in the western United States from 1937 through 1947. The Vancouver group spread and supported information that fostered the adoption of apocalyptic, conspiratorial, and anti-Semitic beliefs.[13]

According to Aho, the connection between Christian Identity and blatant racism could be partly attributed to fundamentalist Protestants from the Midwest Bible Belt and southern states who were fervent vocal proponents of the movement that would eventually become Christian Identity. These individuals included James Lovell, a Texas Baptist; Wesley Swift, an Alabama Methodist; Joe Jeffers, an Alabama Baptist; and Herbert Armstrong, an Iowa Adventist. [14] While Cameron is given credit for being a primary influence in the early development of Christian Identity, Californians Wesley Swift, Bertrand Comparet, and William Porter Gale were also key figures in the early development of Christian Identity in the United States.[15]

Gerald L. K. Smith was a notable national figure in the development of Identity doctrine. Smith was a Church of Christ minister who was an associate of Louisiana political kingpin Huey Long. Characterized as a bombastic and charismatic orator, his extreme ego and political naiveté became apparent (and detrimental) during the unsuccessful presidential campaign of William Lemke. Smith became a friend of Henry Ford's in the late 1930s and received funding from the automobile industry icon for a radio broadcast series. Smith credits Ford for showing him the connection between Judaism and Communism. This focus on the denunciation of both Jews and communism was a prevalent theme during speaking engagements and in his mail order ministry, two businesses that made Smith a millionaire.[16] After World War II, Smith moved to Los Angeles where he became affiliated with anti-Semitic and white supremacists in Southern California. Smith's high profile public appearances included anti-Semitic and racist rhetoric that resulted in the mobilization of opposition minority and Jewish communities in the Los Angeles area.[17]

Wesley Swift, who had been affiliated with the Ku Klux Klan (KKK) in the early 1940s,[18] may have been at least one early source of the Identity hermeneutic that furthered "seed-line" Identity theology. Kaplan provides the following quote in *Radical Religion in America* to indicate how Smith's Identity beliefs were influence by Swift: "He opened the Bible and demonstrated to me with proper text that Christ's worst enemies were not God's chosen people. He identified the 'true Israel' which gave us the Messiah…He demonstrated that the crucifiers of Christ were apostates, sons of Satan, and the seed of Cain."[19]

In addition to Gerald L. K. Smith, Wesley Swift was affiliated with several notable figures influential in the rise of Christian Identity after World War II. Included in this group were Bertrand Comparet, William Gale, and Richard Butler. Comparet was a Stanford educated lawyer and had held the position of deputy district attorney in San Diego. He was an active Christian Identity preacher and was a close associate of Smith. Comparet successfully defended Smith during a 1955 libel suit.[20]

Gale was a former Army lieutenant colonel during World War II who frequently embellished his war record.[21] He was the founder of the Posse Comitatus, a movement he outlined in a 1971 article published in the *Identity Newsletter*. Posse Comitatus was founded on the belief that, constitutionally, no governmental body higher than the county level is legitimate.[22] Gale and his fellow Posse Comitatus followers' refusal to acknowledge state and federal governmental authority resulted in legal complications with the Internal Revenue

Service on tax-related criminal charges. At the time of his death in April 1988, Gale was appealing a 1987 conviction for conspiracy to threaten a judge and an IRS agent. While he preached his anti-Semitic and racial bigotry, Gale kept an enormous secret from his Christian Identity associates: his father was a Jew. The central premise of his Christian Identity beliefs and ministry were based on a complete denial of his heritage.[23]

Posse Comitatus members were responsible for several acts of violence in the Northwest and Midwest during the 1980s. An example of this violence was the 1983 shootout between Gordon Kahl and federal marshals. Kahl, an icon of the radical right and a member of the North Dakota Posse Comitatus, was killed during the incident. Many of the people who later participated in the militia movement were believed to have been involved in the Posse Comitatus groups of this time period.[24] Posse Comitatus members seized an opportunity to spread their message to distressed farmers during the 1980s farm crisis.

Right-wing religious rhetoric may appeal to many people for reasons other than religion. *American Terrorist* by Lou Michel and Dan Herbeck mentions Timothy McVeigh's interest a church near Yellowstone National Park that was involved in stockpiling food and munitions, but their "New Age religious ways failed to trip his trigger." McVeigh was not a believer in organized religion. Instead, he thought natural law guided the universe through a higher power using an internalized method to instill right and wrong in a person.[25] Yet McVeigh attempted to contact Andreas Strassmeir, a German national believed to be staying at the Christian Identity community in Elohim City, Oklahoma, seeking a safe haven after the bombing. McVeigh had met Strassmeir at a gun show. He also attempted to call a representative of the National Alliance to arrange refuge. Neo-Nazi William Pierce, author of *The Turner Diaries*, was the head of the National Alliance.[26] Although he contacted these two groups to seek assistance with escape and sanctuary, McVeigh should not be characterized as a Christian Identity follower or a neo-Nazi.

Richard Butler, a former engineer for Lockheed, had been a member of Swift's California church. Butler moved to Idaho in 1973 and started the Church of Jesus Christ Christian in Coeur d' Alene. His most notable political right-wing activity paralleling the Christian Identity movement was the establishment of the Aryan Nations.[27] Aryan Nations served as a consolidator of right-wing groups, including those who followed Christian Identity doctrine and those who did not follow the movement. Bruce Hoffmann in *Inside Terrorism* describes the Aryan Nations as being "an extremist, anti-Semitic, neo-Nazi group of white supremacists, survivalist and militant tax resisters…"[28] Aryan Nations members were involved in a series of violent acts beginning in the 1980s. These acts included the killing of a Denver, Colorado, Jewish radio talk show host by an Aryan Nations splinter group known as The Order. Members of The Order also committed several armed robberies and bombings during its reign of terror. Butler died in 2004, but not before he saw his Aryan Nations organization financially decimated by a civil judgment.[29] Although Richard Butler's demise appears to have resulted in further fragmentation of the national leadership of the Christian Identity movement, the danger posed by the overall goal of its followers – to establish a racially pure white Aryan country – continues to be a matter of concern.

According to a *CNN.com* article by Henry Schuster, Butler's Aryan Nations successor, August Kries, has offered to form an alliance with al Qaeda. The motive behind the offer is based on common enemies shared by the two extremist groups – the United States government and the Jews. Christian Identity adherents might view involvement with extremist Muslims of Middle Eastern origins as contrary to their core beliefs; Kries dismisses the viewing of al Qaeda members as "mud people" as being "old school racism." He provided the following reassurance to al Qaeda should they become interested in forming an alliance: "the cells are out here and they are already in place. They might not be cells of Islamic people, but they are here and they are ready to fight."[30]

Phineas, a priest mentioned in the Old Testament, has inspired the use of violence in the name of God by a very secretive group of right-wing activists who are Christian Identity followers. According to Hoffman, punishing such violators of divine edicts as homosexuals, inter-racial married couples, and abortionists is the mission of the Phineas Priests. Ending the federal banking system is another divine duty accepted by the Phineas Priests.[31] With the decline of the Aryan Nations, the Phineas Priests have become more prevalent. Phineas Priests are not believed to be an organized group; rather, they appear to be a collection of several individual right-wing extremists who have committed violent crimes in the name of God.[32] In an August 4, 2005 posting on the Aryan Nations website, Pastor Jay Foster described two entities that form the Aryan Nations organization. First is the Aryan Nations proper, which accepts people who may not be religious, but are still attracted to the group because of their "views and systems." The second entity is the biblical wing of the organization, known as the Tabernacles of the Phineas Priesthood.[33] Will the Tabernacles of the Phineas Priesthood actually commit acts of violence in the name of God, as their name implies? The Christian Identity beliefs of its members make potential terrorist acts a constant possibility.

Christian Identity offers devotees explanations for their present deficiencies and reassuring interpretations of the past. The past is described as glorious prior to the theft of their God-given birthright by the evil Jews. As for the future, Christian Identity provides assurances of happiness and global supremacy. Survival in the future is accomplished by the grace of God, through the use of Christian Identity followers' intellect and – alternatively – through the availability of stockpiled food and weaponry.[34]

MILITIAS

The militia movement has evolved during the past three decades, redefining its purposes, ideology, and appeal to future members. Consistent themes include a distrust of the federal government and a belief that citizens will be disarmed by the government. The attraction of the militia movement to prospective members has varied as militias adapt their ideology to address emerging issues.

Militias are part of the informal patriot movement that, according to Matthew Zook, emerged from the challenges (created by the civil rights and feminist movements of the 1960s and 1970s) to the "dominant social and economic systems for regulating race and gender relations."[35] Chip Berlet in *Militia Nation* expands this view of militias when he suggests that militias are a social byproduct of "economic hardship and the partial erosion of traditional structures of white

male heterosexual privilege." He mentions two stresses associated with the "right-wing populist revolt" for which militia members are concerned: first is the stress of the genuine economic suffering that resulted from global restructuring; the second type of stress stemmed from outrage regarding the societal gains achieved by oppressed groups in the United States.[36]

According to a study of threats and reactive mobilizations by Van Dyke and Soule, the increase in the organization of patriot and militia groups is related to economic downturns. These economic hard times resulted in the loss of agricultural and manufacturing jobs.[37]

The loss of land and the heritage of many farmers and ranchers resulted in what rural counselor Glen Wallace referred to in his congressional committee testimony as "community depression." The symptoms of the community depression observed by Wallace are similar to an individual with chronic long-term depression.[38] One of the escape mechanisms for the chronic stress experienced by farmers exhibiting manifestations of depression or psychosis is an outward projection of anger. These individuals want to make those whom they hold responsible feel the pain of the farmers. In the rural crisis of the 1980s, these outward expressions of anger resulted in the murders of bankers and federal lending agents.[39] Wallace acknowledged the violent reaction to the economic crisis in rural America when he stated: "You can't treat human beings in a society the way rural people have been treated without them organizing and fighting back." Involvement in antigovernment right-wing groups became another means for rural Americans to outwardly fight back. [40]

Societal gains by historically oppressed groups, the second area of stress mentioned by Beret, result in the displeasure expressed by many in the patriot movement with regard to unjust advantages extended to minorities and women, specifically nonwhites. Affirmative action programs have become a contentious subject of discourse. Conspiracy theories fueled the anger generated by the societal and economic issues. One tenet of conspiracy theories, mentioned by Beret, is the description of two types of people: parasites and producers. Parasites are viewed by the conspiracy theorist as being at the top and bottom levels of society. The top level contains the corrupt governmental officials and wealthy manipulators of the banks and currency. At the bottom are the aimless, "slacker" parasites who sponge off the hard-working middle class by accepting public assistance. In the middle are the producers, a reflection of the person who typically embraces conspiracy theories. A belief that those at the bottom are mostly blacks and Hispanics injects a racial element into these theories, though in reality welfare and other government relief programs are mostly utilized by whites.[41]

Mark Pitcavage *in Camouflage and Conspiracy*: *The Militia Movement from Ruby Ridge to Y2K*, attributes the rise of participation in militia groups to a variety of incidents that occurred during the 1990s. Included in these events were the passage of the North American Free Trade Agreement (NAFTA), the Brady Bill, the assault rifle ban, the riots in the Los Angeles area after the Rodney King verdict, the presidential election of Bill Clinton, the 1992 Ruby Ridge shootout, and the 1993 Branch Davidian standoff in Waco, Texas.[42] According to the 1999 congressional testimony of former FBI Director Louis Freeh, "most of

the militia movement has no racial overtones and does not espouse bigotry; there are some black and Jewish militia members." While many militia members are not law violators, the presence of Christian Identity followers and individuals who embrace other hate beliefs is an emerging problem.[43]

Militia groups vary in some of their beliefs and priorities, but the preservation of their right to possess and own firearms is universally regarded as the most important issue. Militias view firearms ownership as a means to safeguard against government totalitarianism. Many militia members view, as fact, conspiracy theories based on scenarios where the federal government increases its power gradually and confiscates firearms. Some members believe New World Order conspiracy theories that foreign troops are secretly stationed in the country or staged for an eminent invasion sanctioned by the United Nations.[44]

Timothy McVeigh was not raised on a farm, but his anti-government sentiments could have been partially formed by the disappearance of industrial jobs commonly available to his father's generation. Many of these jobs were lost due to international trade agreements and global economics.[45] His right-wing beliefs were something McVeigh had in common with militia members and other patriot groups. A significant belief opposed the government regulation of the right to own firearms. According to Lou Michel and Dan Herbeck in *American Terrorist: Timothy McVeigh and the Oklahoma City Bombing,* McVeigh belonged to the Ku Klux Klan (KKK) for one year while serving in the U.S. Army. McVeigh determined the Klan's main emphasis was on racism, while his concern was gun ownership rights and patriotism.[46] McVeigh believed politicians had the power to set their own salaries and were able to lavishly reward themselves in violation of the trust the public placed in them. Following his failure to gain employment as a New York toll road collector, despite a high score on the entrance examination, McVeigh surmised he was not hired because he was white and blamed affirmative action programs.[47] The Ruby Ridge incident further inflamed his anger with the federal government to the point where he believed the United States was "becoming an overtaxed police state." Concluding that the National Rifle Association was too weak to protect his second amendment rights, McVeigh canceled his membership.[48] In an interview conducted by a student reporter during the Waco siege, McVeigh claimed the local sheriff was the only person with the legal authority to serve the warrant; federal agents had no authority or legitimate reason to be on Branch Davidian property. McVeigh ultimately found acceptance and understanding among the individuals he associated with while participating in the gun show circuit. He further solidified his belief in a New World Order – a single ruling government in the form of the United Nations – taking over the United States and restricting individual freedom.[49]

Militias, according to Bruce Hoffman in *Inside Terrorism*, come in two varieties. The "talking militias" do not advocate the overthrow of the government and are primarily concerned with preserving the right to bear arms. "Marching militias" or "up-front militias" use force to accomplish their goals. They embrace the more radical anti-Semitic, racist, and subversive principles of the radical right.[50] The Viper militia group in Phoenix, Arizona, is an example of a marching militia: Their members amassed a sizeable stockpile of illegal weapons and practiced the use of explosives. During the investigation following their arrest, the group's plan to bomb buildings in Phoenix was discovered.[51] Closed-cell

militias are mentioned in an article by Martin Lindstedt in the initial issue of the *Modern Militiaman*. Persons wishing to become involved in a militia are only invited to the open militia meetings, never to a closed-cell group. Closed-cell groups are reserved for relatives and trusted friends.[52]

Following the Oklahoma City bombing, reporters portrayed McVeigh as an active militia member.[53] He was not an actual militia member, although he had made an unsuccessful attempt to organize a militia group in Arizona, with his friend Michael Fortier, and publicity after the bombing resulted in an increase in militia activity. Due to the arrests of several militia members in the late 1990s and unfulfilled conspiracy theories related to Y2K, many people left militia organizations. Other individuals left militias because they believed the organizations did not sufficiently address the issues important to them;[54] these were more radical members who probably became affiliated with other right-wing extremist groups that fulfilled their expectations. Others become loners, such as accused Olympic Park bomber Eric Rudolph, and committed violent acts to satisfy their desire for action.[55] Many other members grew bored and lost interest in militias.[56]

After the September 11, 2001 attacks, militias adopted new conspiracy theories to fit their fear of a new world order. Conspiracy theories often provide simplistic analysis, defying explanations of conflict or perceived problems. Militia members who embrace these theories affix blame to individuals or groups, instead of analyzing the complexities of real world issues and power structures.[57] John Trochmann of the Militia of Montana voiced an outlandish conspiracy theory when he claimed Bin Laden was a CIA operative when he masterminded the 9-11 attacks.[58]

Post 9-11 interest in survivalist training and equipment has also been used to increase militia membership and activities. Militia members at a fair in Yakima, Washington actively sought individuals to enroll in classes on terrorism survival. The Militia of Montana sold biological warfare suits, gas masks, and potassium iodide to individuals in various parts of the United States.[59]

Membership in militia organizations has increased and decreased over the past twenty years. Events such as the Oklahoma City bombing and the 9-11 attacks have impacted militia organizations by refocusing their interests. While many militia members are not law violators, the presence of members who have more radical beliefs, such as Christian Identity, is a matter of concern.

SOVEREIGN CITIZENS, FREEMEN, AND COMMON LAW COURTS

People involved in groups referring to themselves as "sovereign citizens," "freemen," and "common law court members" are categorized as "separatist" by Leonard Weinberg, Elizabeth Francis, and Randall Lloyd in their article "Courts Under Threat." In addition to a formative relationship with Christian Identity, a manuscript known as the *Nehemiah Township Document and Common Law Contract* provides the foundation for separatist organizations. In 1982, twenty-eight people signed the document that was subsequently notarized and filed by the county clerk in Kootenai County, Idaho. Notable extremist signatories included Richard Butler and KKK Imperial Wizard Thom Robb.[60] A religiously-based Republican government, in which only Aryan freemen would have rights, was the ultimate goal of the *Nehemiah Township Charter*. It referred to God's

divine laws as the only laws applicable to Aryans. National Courts consisting of seventy judges would be established to hand down verdicts according to God's law. The National Courts and lesser-affiliated judicial bodies would have overriding authority over other political entities, including state and federal court systems. Those persons who were not Aryan freemen would have no rights to participate in government or in the legal system. As in the Posse Comitatus movement, county government provides the structure for posses to function, though charters would be created as a new entity in government. Township citizens would have the power not to abide by any ordinance, regulation, or law enacted by municipal, state, or federal governmental bodies. This power also includes the right to ignore the federal tax code. The *Charter* contains references to the United States Constitution and English common law. One of the final passages in the *Charter* makes reference to an attack on one member being the equivalent to an attack on the whole group. This reference reveals that the signers realized the rebellious nature of their actions and beliefs – an indicator of future actions by some of the signers, who were subsequently convicted and incarcerated for their violent activities.[61]

In addition to the information contained in the *Nehemiah Township Charter*, Richard Abanes' book, *American Militias*, describes characteristics of separatists' beliefs. Included in these beliefs are two types of citizenship. State citizenship is considered natural and is believed to have been present before the ratification of the Fourteenth Amendment. The other form of citizenship is conferred by the Fourteenth Amendment and the Bill of Rights; in this form, citizens are obligated to comply with federal statutes, regulations, codes, judgments and rulings. Separatists believe the blood relatives of state citizens may reclaim inherited sovereign citizenship by breaking implicit contracts binding them to the federal government and its inferior form of citizenship. Birth certificates, marriage licenses, Social Security cards, and driver and vehicle licenses are examples of unlawful contracts to be broken to regain sovereignty. Sovereign citizens are not required to follow federal law, but are required to adhere to common law court judgments.[62]

Two other idiosyncratic separatist beliefs worthy of mention are claims that the United States Constitution was suspended in 1933 by the War and Emergency Powers Act and the Sixteenth Amendment was not properly ratified, thereby nullifying the legality of the federal income tax system. In the late 1990s, several common law courts were formed, predominantly in West and Midwest states. Common law activities included bogus liens filed against the property of judges, law enforcement officers, and other public officials. Illegitimate common law arrest warrants were issued for public officials who made decisions or rulings against the edict of separatists.[63] A decline in occurrences of separatist activities in the early twenty-first century is partly attributed to new laws that addressed the common law court activities.[64]

During the summer of 1997, Weinberg, Francis, and Lloyd conducted a random survey of 3,000 judges who had experience with separatists. Survey results revealed most judges viewed the separatists as being "angry individuals who are bright enough to have absorbed some abstract interpretation to explain their circumstances but who still lack the capacity, often provided by education,

to place the interpretation in a broader or comparative framework of understanding." Of the judges who had encountered separatist challengers, over half indicated traffic cases were the most frequently disputed. A prevalence of cases involving weapons offenses was not surprising due to the Second Amendment issues embraced by militia members. Additionally, frequently disputed episodes involving domestic abuse, child custody, and alimony issues were viewed by Weinberg, et al. as indicative of the high stress associated with extremist political behavior.[65] The emotional vehemence of separatists is revealed in the survey results: Twenty-seven percent of the judges who reported challenges indicated they had received threats of violence. Four judges reported being victims of physical assaults.[66]

KU KLUX KLAN

The KKK is the domestic 'granddaddy' of the right-wing extremist movement. It was founded in Pulaski, Tennessee, between late December 1865 and June of 1866, at the beginning of the Reconstruction era following the Civil War. The name of the organization is derived from the Greek word *kuklos*, which translates to English as "circle." The group changed the Greek word slightly to kuklux and added the word klan to the ending to note the Scottish heritage of the group's organizers. Six former confederate soldiers created the organization as a non-political social club for the amusement of themselves and other community members. In the beginning, the white sheets and elaborate costumes worn by the Klansmen were referred to as costumes of mystique and amusement. The amusement eventually transformed into intimidation. Klansmen also believed their white, hooded costumes represented the ghosts of dead confederate soldiers coming back to cast retribution upon the inferior Negro race.[67] This activity eventually led to freed blacks and white carpetbaggers from the North becoming the targets of degrading and frequently vicious nocturnal raids, often resulting in acts of violence and murder.[68] The Klan dens spread throughout Tennessee and eventually to Mississippi and Alabama. The Klan's first national convention was held in Nashville, Tennessee, in 1867, where Confederate General Nathan Forrest became the first elected grand wizard. Forrest officially dissolved the Klan in 1869, but the activities of the various dens throughout the South continued.[69]

The first legislation designed to fight the intimidation and violence inflicted by members of the Klan was passed in 1870. The new law was designed to enforce the Fifteenth Amendment to the Constitution by outlawing interference with voting rights through intimidation, bribery, or use of force. Passage of this act resulted in an increased rate of Klan violence in the south during the 1870 elections.[70] In 1871, continued Klan violence resulted in President Ulysses S. Grant pushing Congress to pass the Ku-Klux Klan Bill: This law allowed any citizen of the United States to seek a federal judicial remedy for the violation of constitutional rights. Persons with foreknowledge of Klan violence were held liable for victims' suffering. A provision of the bill made conspiring by two or more persons to violate another person's rights a crime. The boldest parts of the Ku-Klux Klan Bill allowed the president to suspend temporarily the writ of habeas corpus and use federal troops to quell civil unrest aimed at depriving anyone from exercising their constitutional rights.[71] As racist, southern, white

conservatives regained legitimate power from the Reconstruction governments established at the end of the Civil War, the Klan faded from prominence.[72]

The Klan was reinvigorated in 1915, by the D. W. Griffith motion picture *Birth of a Nation,* which was based on Thomas Dixon's novel *The Clansmen*.[73] The movie glorified the Klan of the Reconstruction Era as saviors and portrayed a black man as the rapist of a frail innocent white girl.[74] The ceremonial burning of crosses was first depicted in the novel and was portrayed in the movie. Interest in the KKK intensified as Klansmen used movie showings to promote the organization.[75] The born-again Klan was less violent than the original Klan, but added the hatred of Jews and Catholics to the traditional hatred of blacks. Klan membership throughout the country was estimated to have been in the millions during the 1920s and 1930s. Prior to and during World War II, Klan membership continued to dwindle, only to rebound again during the turbulent civil rights movement of the 1960s. The Klan does not currently have a nationwide central governing organization; it consists of several, unconnected groups using variations of the Klan moniker. In keeping with the multiple affiliation characteristics of right-wing members, some members of Klan groups are followers of the Christian Identity movement.[76]

NEO-NAZIS

Neo-Nazis, as the name implies, are the new followers of Nazi ideology. Members of this movement embrace many of the World War II Nazi symbols, including the swastika, which is considered the icon of the movement. Neo-Nazis refer to themselves as National Socialists and hold Adolph Hitler in high regard,[77] but they do not follow completely the ideas of Hitler's Nazi party. The modern rendition of these groups can be divided into three categories: followers of Odinism, Christian Identity believers, and groups embracing other spiritual or religious notions.[78] Christian Identity believers associated with the neo-Nazi movement have been discussed earlier and included Richard Butler's Aryan Nations groups, now lead by August Kries.

Believers of Odinism and Ásatrú reject Christianity,[79] but adopt the reconstructed beliefs of the pre-Christian mythical Norse gods of the Vikings. To attract followers who may already have multiple systems of religious or philosophical beliefs, Odinists use ritual magic, fraternal camaraderie, and a flexible ideology. Through the influences of Rud Mills (1930s) and Else Christensen (1960s), marked differences have emerged between Odinism and Ásatrú. First, individuals who embrace Odinism are more in touch with right-wing white supremacy adherents. Most Ásatrú followers reject such associations. Next, Odinists accept the validity of conspiracies when viewing the events of history, while most Ásatrú followers do not embrace these theories. A third difference is the warrior principle that drives Odinists to consider forceful retaliation for perceived past injustices by the dominant culture. A fourth difference is that Odinists hold racist feelings and opinions, which frequently merge with racial mysticism. Last, Odinism places an emphasis on the oversimplification of complex information associated with the revitalized tribal ideas of the Vikings. Ásatrú followers do not accept efforts to simplify their reconstruction of the communal, magical, and religious practices as they apply to modern society.

Many individuals who were involved in the rise of Hitler's Third Reich were known to have been Odinists.[80]

George Lincoln Rockwell started the American Nazi Party (ANP) in 1958; the organization was later called the National Socialist White People's Party. The need for white people to take back the country from the minorities, aliens, and terrorists was one of Rockwell's beliefs. Betty Dobratz and Stephanie Shanks-Meile, in their book *White Power, White Pride!,* mention Rockwell's advocacy of worldwide white power as a means to stop the mongrelization of the white race. A recently-expelled group member killed Rockwell in 1967.[81] William Pierce, a former Oregon State University physics instructor and member of Rockwell's ANP, later established and directed the National Alliance.[82]

Pierce is also the creator of Cosmotheism, a religious belief described by Brad Whitsel in *Aryan Visions for the Future in the West Virginia Mountains* as centered upon the "deterministic ideas reflecting the 'unlimited destiny' of the white race." The Cosmotheist believes an evolutionary force, still guiding us today, created the races. According to Pierce's view, the white race maintains a special status due to its past historical achievements, which far surpass the accomplishments of other races.[83] Placing man on a course to achieve godhood was what Pierce described as the divine mission of Cosmotheism. Some elements of Odinism have been incorporated into Cosmotheism, such as Norse legends and the use of mysterious runes, ancient characters used in Anglo-Saxon, Scandinavian, or Teutonic writings.[84]

Pierce wrote *The Turner Diaries* under the pseudonym Andrew McDonald in 1978. The novel described the revolution against an evil federal government with established race-mixing, gun control, and other detestable actions. *The Turner Diaries* was believed to have inspired Robert Mathews to establish the violent white supremacist group known as The Order.[85] Timothy McVeigh also was inspired by *The Turner Diaries:* In an envelope found in the car driven from Oklahoma City after the bombing, McVeigh had placed articles he wanted to be discovered upon his capture. Among the items was a paper with the following quotes from Earl Turner, the central character of *The Turner Diaries*:

> The real value of our attacks today lies in the psychological impact, not in the immediate casualties. More important though, is what we taught the politicians and the bureaucrats. They learned this afternoon that not one of them is beyond our reach. They can huddle behind barbed wire and tanks in the city, and they can hide behind the concrete walls of their country estates, but we can still find them and kill them.[86]

After Pierce's July 2002 death, Erich Gliebe, the former boxer known as The Aryan Barbarian, assumed the National Alliance leadership position. As is frequently the case in right-wing groups, disagreement among the other potential leaders of the group resulted in resignations or expulsions from the National Alliance. This disarray in the American neo-Nazi movement has resulted in one of Pierce's intellectual protégés, Kevin Strom, forming the National Vanguard and another Pierce follower, Billy Roper, starting the group known as White Revolution.[87]

Rex (Gerhard) Lauck, known as the Farm Belt Fuhrer,[88] is described by Ingo Hasselbach in *Fuhrer-Ex* as being an international neo-Nazi leader. Based in

Lincoln, Nebraska, Lauck is the leader of the NSDAP/AO, the "National Socialist German Workers' Party/Aufbau ("building up" in German) and Auslands ("abroad") Organization. Lauck's NSDAP/AO was patterned after the organization of the same name formerly operated by the Third Reich. Lauck had a significant influence on the activities and advancement of neo-Nazi activities in Germany and other European countries. His connections with old Nazis in South America helped to finance neo-Nazi activities.[89] Lauck's publishing business in Lincoln produced and distributed a variety of Nazi paraphernalia, such as bumper stickers, books, videos, and computer games.[90] Lauck's power was sufficient to order acts of terrorism against various officials associated with the attempt to host the Olympics in Berlin. His rationale for ordering the acts of terrorism was to deny the Federal Republic of Germany the chance to eclipse the Olympics hosted by the Third Reich prior to World War II. Acts of terrorism by neo-Nazis and left-wing elements resulted in Germany abandoning efforts to host the Olympics.[91] Eventually, Lauck was arrested in Denmark and charged with distributing terrorist materials and Nazi propaganda.[92]

SKINHEADS

The terrorist youth subculture label has been used to describe the groups popularly known as the skinheads.[93] Skinheads first materialized in London during the 1960s as a working-class youth response to the hippie trend.[94] These early skinheads, according to Mark Hamm in *American Skinheads: The Criminology and Control of Hate Crime,* combined the cultures of the working-class white and the Jamaican black immigrant. Their shaved heads symbolized their visibly defiant self-determination and served as a practical advantage by preventing opponents from grabbing their hair during street fights. These early skinheads targeted for their acts of violence Pakistanis, hippies, homosexuals, and students from upper-class families who attended Cambridge and the London School of Economics. In 1972, Scotland Yard successfully cracked down on skinheads perpetrating violent acts against innocent victims, thereby curtailing skinhead activities.[95]

Second-generation skinheads in Britain reemerged as a problem in 1981 as Ian Stuart, leader of the band Skrewdriver, formed a political action group called White Noise. The combination of politics and music led to an affiliation with the British National Front, a right-wing, neo-fascist organization. Resurgence of skinhead racial violence was encouraged further by anti-immigrant and nationalistic views expressed by officials in the Thatcher administration.[96] Skrewdriver's popularity as the premier British white power band eventually led to a record contract with West German record company Rock-O-Rama Records. This contract resulted in their white hate, neo-Nazi, skinhead message being distributed throughout Europe, the United States, and Canada. The popularity of white power rock music was a factor in the development of the skinhead movement into an international youth subculture.[97]

According to J. Cotter, in *Sounds of Hate: White Power Rock and Roll and the Neo-Nazi Skinhead Subculture,* the propagation, persistence, and viability of the skinhead culture can be attributed to the messages communicated in the lyrics of white power rock and roll. This music validates the use of violence against non-

white immigrants perceived as a threat to the white race and the skinhead culture. In addition to being a source of entertainment for skinheads, white power rock and roll music has been a vehicle for the distribution of racist propaganda to a wide group of listeners. White power bands travel to various countries to give concerts and spread the skinhead way of life and ideology. The worldwide skinhead publication and music distribution network provides support to the bands and facilitates the flow of information to any interested persons.[98] A significant segment of the white power music and publication network is represented by Resistance Records and *Resistance Magazine*. George Eric Hawthorne, alias George Burdi, the lead singer of the band RAHOWA (Racial Holy War), founded Resistance Records in 1993. The publication side of the business doubled as a fan magazine for white power bands and a propaganda tool for white supremacy. Following Hawthorne's arrest for violating the Canadian law prohibiting the distribution of hate material, and his difficulties in the United States related to tax irregularities, Resistance Records fell on hard times. Eventually, it was purchased by Willis Carto and Todd Blodgett and later sold to William Pierce of the National Alliance. Pierce also acquired a competing Swedish white power music distributor to further bolster his business.[99] Prior to his death in 2002, Pierce had capitalized upon his investment through Internet sales and distribution of hate music, computer games, and literature.[100]

Clark Martell, a Skrewdriver follower and American Nazi Party member from Blue Island, Illinois, formed the first American skinhead group. A crime spree in the Chicago area was attributed to Martell and his skinhead group. Their violence resulted in the assault of six Hispanic women, swastikas painted on the walls of three synagogues, and other damage to Jewish-owned businesses. Martell's incarceration for the crime spree neutralized the skinhead movement in the Chicago area. Robert Heick formed a second group of skinheads in the Haight-Ashbury district of San Francisco. They adopted the typical appearance of the skinhead movement: Levi jeans, red suspenders, Fred Perry shirts, and Doc Martens steel-toed boots. Heick also adorned his body with sixteen tattoos of Vikings, swastikas, and eagles. Following a brief crime spree, Haight-Ashbury business owners persuaded police to crack down on the skinheads. Heick's group was neutralized, but many other skinheads would later emerge in the Bay area.[101]

Skinheads are considered the foot soldiers of the right-wing movement and are the target of recruitment efforts by other right-wing organizations, such as the Aryan Nations, KKK groups, and Church of the Creator (COC).[102] Thomas Metzger's White Aryan Resistance (WAR), an organization known for using television for recruitment, successfully enlisted skinheads into his organization. Skinhead WAR members were linked to the 1988 murder in Portland, Oregon of an immigrant from Ethiopia and the assault of three other immigrants. A civil case related to the wrongful death of the immigrant resulted in a $12.5 million judgment against WAR.[103]

According to a 2006 Anti-Defamation League (ADL) press release, skinhead activity has increased along with a rise in hate crimes against African-Americans, Hispanics, immigrants, and homosexuals. The ADL attributes four factors to the increase in skinhead activity. First, alienated or disaffected youth are cordially invited to join the skinhead social network of hate on the Internet. Second, white

power music glorifying the skinhead movement is thriving. Third, the global expansion of the Hammerskin Nation and other skinhead groups through the Internet has resulted in the expansion of other white supremacist sites and has enhanced the ability of skinheads to communicate with each other. Finally, the level of competition from other white supremacist groups has been reduced by the deaths or arrests of their leaders and a resulting leadership vacuum characterized by group infighting.[104]

CONCLUSION AND FUTURE TRENDS OF THE RADICAL RIGHT

Miki Vohryzek-Bolden lists future trends of the radical right in *Right-Wing Terrorists and the Threats They Pose for Americans in the 21st Century*. The first trend is the right-wing shift from group affiliations to individual actors.[105] Louis Beam, a former Texas KKK grand dragon and participant in the Aryan Nations, is associated with promoting the concept of leaderless resistance. In his essay "Leaderless Resistance," Beam advocates the use of individuals or autonomous small groups, also known as cells, to perform acts of violence. Leaderless resistance is a means of avoiding the perceived pitfalls of the military model of organization. The unlinked cells and individuals make detection, information gathering, and informant development difficult.[106] One example of leaderless resistance was the involvement of Timothy McVeigh, Terry Nichols, Michael Fortier, and Lori Fortier in the Oklahoma City bombing. Use of leaderless resistance increases the need for effective long-term undercover officers to gather intelligence and be vigilant for signs of radical cells or lone wolf terrorists. Undercover officers must gain sufficient trust to be included in the more secure and exclusive gatherings where terrorist actions are likely to be discussed and planned or more radicalized individuals identified.

Other future trends of right-wing groups mentioned by Vohryzek-Bolden are attempts to have right-wing ideas and images assimilated into mainstream politics, and a rise in Odinism, white power rock music, and the influence of neo-Nazi groups. The desire of some group members to acquire weapons of mass destruction is mentioned as another future trend.[107] The confiscation in 2004 of a cyanide compound belonging to William Krar and his common-law wife Judith Bruey is an example of this potentiality becoming reality.[108] An additional trend involves the continued refinement of communications networks on the Internet, resulting in a potential ability to connect extremist and terrorists groups throughout the world. Related to this trend is the globalization of terrorist and extremist groups, including their symbols, religions, and music. Two final trends described by Vohryzek-Bolden include the formation of a more hard-core group of "true believers" and the recruitment of college-educated individuals who are more articulate and capable of handling the duties of group spokespersons.[109]

To safeguard our nation from future acts of terrorism, a constant awareness of right-wing extremist beliefs, activities, and adherents must be maintained. Public safety officials must be aware of the heroes and martyrs of the radical right and the catalytic events that may result in future acts of terrorism. Individuals committing criminal activities associated with the proliferation of right-wing extremist activities must be investigated and, if sufficient evidence is present, effectively adjudicated. The threat posed by the radical right may seem dormant, but the ideas

that promote violence against the government and other perceived enemies remain a constant danger. Developing sufficient and timely intelligence will be important in avoiding future catastrophic incidents of terrorism perpetrated by right-wing extremists.

Captain Timothy G. Baysinger *is a twenty-eight year veteran of the Missouri State Highway Patrol and currently serves as the director of the Research and Development Division. His administrative duties have included staff inspections, strategic planning, property/evidence coordination, law enforcement accreditation, and assessment center management. Captain Baysinger recently completed his master degree work at the Naval Postgraduate School's Center for Homeland Defense and Security.*

---

[1]Jeffrey Kaplan, "Right Wing Violence in North America," *Terrorism and Political Violence* 7, no. 1 (1995): 46.

[2] The World Church of the Creator, now known as the Creativity Movement is one group that does not embrace Christian Identity. According the Anti-Defamation League (ADL) Law Enforcement Agency Resource Network website, [http://www.adl.org/learn/Ext_US/WCOTC.asp?xpicked=3&item=17], the Creativity Movement does not embrace beliefs normally associated with religion. Creativity Movement followers view their religion as revolving around the supremacy of the white race over all other races. Another right-wing group not embracing the beliefs of Christian Identity is the The National Alliance. Their religion was formulated by William Pierce, and is called Cosmotheism. According to Brad Whitsel's essay "Aryan Visions for the Future in the West Virginia Mountains" in *Terrorism and Political Violence* (Winter 1995): 117, Cosmotheism is "characterized by an idiosyncratic blend of ideas including Darwinian evolution, Teutonic mythology, and 'scientific' findings of early racial theorists..." Included in the beliefs of Cosmotheists are ideas related to their racial preordained future and their elevation to Aryan Godness.

[3] David W. Brannan, "Left- and Right-wing Political Terrorism," in *The Politics of Terrorism*, Andrew Tan, ed. (London: Europa Publications, 2006), 57.

[4] Ibid.

[5] Peter Peters, "Special Report - Framing Deceit: An Analysis by Pastor Peter J. Peters of a Speech to the National Press Club by a Spokesperson of the So-Called 'Southern Poverty Law Center'." [http://www.scripturesforamerica.org/PDF%20Files/Framing%20Deceit.pdf]. February 2006.

[6] Bertrand Comparet, "Christian Identity: What is it?" [http://www.churchoftrueisrael.com/comparet/what-is-identity.html]. February 2006.

[7] Arthur Koestler, *The Thirteenth Tribe,* First American ed. (New York, NY: Random House, 1976), 17.

[8] Ibid., 13.

[9] Ibid., 15-17.

[10] Michael Barkun, *Religion and the Racist Right: The Origins of the Christian Identity Movement* (Chapel Hill, NC: University of North Carolina Press, 1997), 4.

[11] James A. Aho, *The Politics of Righteousness: Idaho Christian Patriotism* (Seattle and London: University of Washington Press, 1990), 52.

[12] The Anti-Defamation League, "The International Jew: Anti-Semitism from the Roaring Twenties Revived on the Web," [http://www.adl.org/special_reports/ij/dearborn_independant.asp]. February 2006.

[13] Barkun, *Religion and the Racist Right*, 51.

[14] Aho, *Politics of Righteousness,* 3.

[15] Jeffrey Kaplan, *Radical Religion in America: Millenarian Movements from the Far Right to the Children of Noah* (Syracuse, NY: Syracuse University Press, 1997), 3.

[16] Glen Jeansonne, "Gerald L. K. Smith: From Wisconsin Roots to National Notoriety," *Wisconsin Magazine of History* 86, no. 2 (2002-2003): 24-26.

[17] David J. Leonard, "The Little Fuehrer Invades Los Angeles: The Emergence of a Black-Jewish Coalition after World War II," *American Jewish History* 92, no. 1 (2004): 88.
[18] Daniel Levitas, *The Terrorist Next Door: The Militia Movement and the Radical Right* (New York, NY: St. Martin's Griffin, 2004), 23.
[19] Kaplan, *Radical Religion in America,* 3-4.
[20] Barkun, *Religion and the Racist Right,* 60.
[21] Levitas, *Terrorist Next Door,18-19*
[22] Ibid., 108-109.
[23] Ibid., 295-298.
[24] Bruce Hoffman, *Inside Terrorism* (New York, NY: Columbia University Press, 1998), 110.
[25] Lou Michel and Dan Herbeck, *American Terrorist: Timothy McVeigh and the Oklahoma City Bombing,* 1st ed. (New York, NY: Regan Books, 2001), 142-143.
[26] Ibid., 225.
[27] Barkun, *Religion and the Racist Right,* 68-70.
[28] Hoffman, *Inside Terrorism,*113.
[29] Jonathan Martin, "Richard Butler, Who Led Aryan Nations, Dies in Idaho at 86." [http://archives.seattletimes.nwsource.com/cgi-bin/texis.cgi/web/vortex/display?slug=butlerobit09m&date=20040909&query=richard+butler+aryan+nations+dies]. February 2006.
[30] Henry Schuster, "An Unholy Alliance: Aryan Nation Leader Reaches Out to al Qaeda." [http://www.cnn.com/2005/US/03/29/schuster.column/index.html]. February 2006.
[31] Hoffman, *Inside Terrorism,* 119.
[32] Anti-Defamation League, "Breakup of Aryan Nations Leads to Formation of Successor Groups," [http://www.adl.org/learn/extremism_in_america_updates/groups/aryan_nations/Aryan_nations_break_up.htm]. February 2006.
[33] Jay Faber, "From the Desk of Pastor Jay Faber," [http://www.agentofchaos.invisionzone.com/index.php?showtopic=1447]. February 2006.
[34] Kaplan, "Right Wing Violence in North America," 52.
[35] Matthew Zook, "The Unorganized Militia Network: Conspiracies, Computers, and Community," *Berkeley Planning Journal* 11 (1996): 27.
[36] Chip Berlet and Matthew N. Lyons, "Militia Nation," *The Progressive* 59, no. 6 (1995): 22-25.
[37] Nella Van Dyke and Sarah A. Soule, "Structural Social Change and the Mobilizing Effect of Threat: Explaining Levels of Patriot and Militia Organizing in the United States," *Social Problems* 49, no. 4 (2002): 509.
[38] Joel Dyer, *Harvest of Rage: Why Oklahoma City is Just the Beginning* (Boulder, CO: Westview Press, 1997), 64.
[39] Ibid., 39.
[40] Ibid., 64-65.
[41] Berlet and Lyons, "Militia Nation," 24-25.
[42] Mark Pitcavage, "Camouflage and Conspiracy: The Militia Movement from Ruby Ridge to Y2K," *American Behavioral Scientist, Special Issue: Terrorism in the 21st Century* 44, no. 6 (2001): 961.
[43] Louis J. Freeh, "Testimony of Louis J. Freeh, Director, FBI Before the Senate Committee on Appropriations Subcommittee for the Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies." [http://www.fas.org/irp/congress/1999_hr/990204-freehct2.htm]. February 2006.
[44] Pitcavage, "Camouflage and Conspiracy," 964-965.
[45] Dyer, *Harvest of Rage,* 221.
[46] Michel and Herbeck, *American Terrorist,* 89.
[47] Ibid., 99-100.
[48] Ibid., 108-111.
[49] Ibid., 120-122.
[50] Hoffman, *Inside Terrorism,* 107-108.
[51] Patricia King and Randy Collier, "Vipers in the Burbs," *Newsweek* 128, no. 3 (1996): 20-24.
[52] Martin Lindstedt, "Forming In-fill-Traitor Resistant Patriot Organizations." [http://users.mo-net.com/mlindste/mmmisu1.html]. February 2006.
[53] Chip Berlet, "Militias in the Frame," *Contemporary Sociology* 33, no. 5 (2004): 517.

[54] Anti-Defamation League, "The Quiet Retooling of the Militia Movement." [http://www.adl.org/extremism/Militia/Militia_retools.pdf]. February 2006.
[55] Christopher Hewitt, *Understanding Terrorism in America: From the Klan to al Qaeda* (London and New York, NY: Routledge, 2003), 78.
[56] Andrew Wolfson and John Masson, "Militias Dwindle Since Oklahoma City Bombing." [http://www.usatoday.com/news/nation/2001-04-23-mcveigh-militias1.htm]. February 2006.
[57] Political Research Associates, "Challenging Populist Conspiracism." [http:www.publiceye.org/tooclose/cons_not.html]. February 2006.
[58] Craig Welch, "Militia Groups See a Revival." [http://archives.seattletimes.nwsource.com/cgi-bin/texis.cgi/web/vortex/display?slug=militia16m0&date=20011016&query=militia+groups+see+a+revival]. February 2006.
[59] Ibid.
[60] Leonard B. Weinberg, Elizabeth Francis, and Randall D. Lloyd, "Courts Under Threat," *Terrorism and Political Violence* 11, no. 2 (1999): 94.
[61] Michael Barkun, "Violence in the Name of Democracy: Justifications for Separatism on the Radical Right," *Terrorism and Political Violence* 12, no. 3/4 (2000): 197-198.
[62] Richard Abanes, *American Militias* (Downers Grove, IL: InterVarsity Press, 1996), 11.
[63] Ibid., 95-96.
[64] Miki Vohryzek-Bolden, "Right-Wing Terrorists and the Threats They Pose for Americans in the 21st Century," *Humboldt Journal of Social Relations* 27, no. 2 (2003): 71.
[65] Weinberg, Francis, and Lloyd, *Courts Under Threat,* 99-100.
[66] Abanes, *American Militias,* 103.
[67] Wyn Craig Wade, *The Fiery Cross: the Klu Klux Klan in America* (New York, New York: Simon and Schuster, 1987), 31-35.
[68] Ibid., 46.
[69] Betty A. Dobratz and Stephanie L. Shanks-Meile, *"White Power, White Pride!": The White Separatist Movement in the United States* (New York, NY: Twayne Publishers, 1997), 37.
[70] Wade, *Fiery Cross,* 83
[71] Ibid., 90.
[72] Mark Pitcavage, *The Investigator's and Prosecutor's Guide to Common Terms Used by Antigovernment Extremists,* 2nd ed. (Tallahassee, Florida: Institute for Intergovernmental Research, 1999), 55.
[73] Ibid., 55.
[74] Wade, *Fiery Cross,* 130.
[75] Ibid., 146-147.
[76] Pitcavage, *Investigator's and Prosecutor's Guide,* 55.
[77] John George and Laird Wilcox, *American Extremists: Militias, Supremacists, Klansmen, Communists, and Others* (Amherst, New York: Prometheus Books, 1996), 323
[78] Pitcavage, *Investigator's and Prosecutor's Guide,* 75.
[79] Kaplan, *Radical Religion in America,* 25.
[80] Ibid., 15-17.
[81] Dobratz and Shanks-Meile, *"White Power, White Pride!",* 58.
[82] Kaplan, *Radical Religion in America,* 34-35.
[83] Brad Whitsel, "Aryan Visions for the Future in the West Virginia Mountains," *Terrorism and Political Violence* 7, no. 4 (1995): 123.
[84] Ibid., 128-129.
[85] Ibid., 121.
[86] Michel and Herbeck, *American Terrorist*, 228.
[87] T. K. Kim, "The Wannabe," *Intelligence Report* , no. 119 (2005): 13.
[88] Ingo Hasselbach and Tom Reiss, *Fuhrer-Ex: Memoirs of a Former Neo-Nazi,* First ed. (New York, NY: Random House, Inc., 1996), 383.
[89] Ibid., 161.
[90] Ibid., 163.
[91] Ibid., 296-297.
[92] Ibid., 383.

[93] J. Cotter, "Sounds of Hate: White Power Rock and Roll and the Neo-Nazi Skinhead Subculture," *Terrorism and Political Violence* 11, no. 2 (1999): 137.
[94] Randy Blazak, "White Boys to Terrorist Men: Target Recruitment of Nazi Skinheads," *American Behavioral Scientist* 44, no. 6 (2001): 985.
[95] Mark S. Hamm, *American Skinheads: The Criminology and Control of Hate Crime,* First ed. (Westport, CT: Praeger, 1993), 24-27.
[96] Ibid., 31-33.
[97] Ibid., 35.
[98] Cotter, "Sounds of Hate," 134-135.
[99] Anti-Defamation League, "Deafening Hate: The Revival of Resistance Records." [http://www.adl.org/resistance%20records/print.asp]. February 2006.
[100] Anti-Defamation League, "National Alliance." [http://www.adl.org/learn/ext_us/N_Alliance.asp]. February 2006.
[101] Hamm, *American Skinheads*, 38-42.
[102] Dobratz and Shanks-Meile, *"White Power, White Pride!,"* 69.
[103] Pitcavage, *Investigator's and Prosecutor's Guide,* 119.
[104] Anti-Defamation League, "ADL Reports Resurgence of Racist Skinheads in U.S. and Launches New Online Racist Skinhead Project." [http://www.adl.org/PresRele/NeoSk_82/4860_82.htm]. February 2006.
[105] Vohryzek-Bolden, "Right-Wing Terrorists," 91.
[106] Louis Beam, "Leaderless Resistance." [http://www.louisbeam.com/leaderless.htm]. February 2006.
[107] Vohryzek-Bolden, "Right-Wing Terrorists," 91.
[108] "Cyanide, Arsenal Stirs Domestic Terror Fear," Available from [http://www.cnn.com/2004/US/Southwest/01/30/cyanide.probe.ap]. February 2006.
[109] Miki Vohryzek-Bolden, "Right-Wing Terrorists," 91.

Lessons We Don't Learn: A Study of the Lessons of Disasters, Why We Repeat Them, and How We Can Learn Them

Amy K. Donahue and Robert V. Tuohy

On February 23, 2006, in a press conference to release the White House report on lessons learned from Hurricane Katrina, Assistant to the President for Homeland Security and Counterterrorism Frances Townsend said "[The president] demanded that we find out the lessons, that we learn them and that we fix the problems, that we take every action to make sure America is safer, stronger and better prepared." The lessons Townsend called out in her briefing concerned planning, resource management, evacuation, situational awareness, communications, and coordination. No one in the emergency response community was surprised. We know these are the problem areas. We knew they would be before Katrina ever hit the Gulf coast. Why? Because we identify the same lessons again and again, incident after incident.

In fact, responders can readily predict the problems that will arise in a major incident and too often their predictions are borne out in practice. Even a casual observer can spot problems that recur: communications systems fail, command and control structures are fractured, resources are slow to be deployed. A quick perusal of the reports published after the major incidents of the past decade quickly shows this to be true. Consider the following:

> **Hurricane Katrina, 2005**
> In terms of the management of the Federal response, our architecture of command and control mechanisms as well as our existing structure of plans did not serve us well. Command centers in the Department of Homeland Security (DHS) and elsewhere in the Federal government had unclear, and often overlapping, roles and responsibilities that were exposed as flawed during this disaster…This lack of coordination at the Federal headquarters-level reflected confusing organizational structures in the field…Furthermore, the JFO [Joint Field Office] staff and other deployed Federal personnel often lacked a working knowledge of NIMS [the National Incident Management System] or even a basic understanding of ICS [Incident Command System] principles.
> – From *The Federal Response to Hurricane Katrina Lessons Learned*, 2006: 52

> **September 11 attack, 2001**
> It is a fair inference, given the differing situations in New York City and Northern Virginia, that the problems in command, control, and communications that occurred at both sites will likely recur in any emergency of similar scale. The task looking forward is to enable first responders to respond in a coordinated manner with the greatest possible awareness of the situation…Emergency response agencies nationwide should adopt the Incident Command System (ICS).When multiple agencies or multiple jurisdictions are involved, they should adopt a unified command. Both are proven frameworks for emergency response.
> – From *The 9/11 Commission Report*, 2004: 315, 397

> **Oklahoma City bombing, 1995**
> The Integrated Emergency Management System (IEMS) and Incident Command System (ICS) were weakened early in the event due to the immediate response of

> numerous local, state and federal agencies, three separate locations of the Incident Command Post (ICP), within the first few hours, and the deployment of many Mobile Command Posts (MCPs), representing support agencies.
> – From the *After Action Report: Alfred P. Murrah Federal Building Bombing*, 2003: 3

> **Hurricane Andrew, 1992**
> The Committee heard substantial testimony that the post-disaster response and recovery to Hurricane Andrew suffered from several problems, including: inadequate communication between levels of government concerning specific needs; lack of full awareness of supply inventories and agency capabilities; failure to have a single person in charge with a clear chain of command; and inability to cut through bureaucratic red tape.
> – From the *Governor's Disaster Planning and Response Review Committee Final Report*, 1993: 60

As these statements reveal, we repeatedly confront command and control issues in large incidents. These are but a few examples from dozens of reports that cite the need for sound command structures. Somehow, though, we fail to *learn* this and other crucial lessons that have been identified in after-action reports for decades. The central concerns of this paper are why that is so and how we can improve. We report here on an exploratory investigation that targets six research questions.

1. Is it true that lessons recur?

2. What lessons are persistently identified?

3. Why do these lessons continue to be identified as important?

4. Why are these lessons so hard to learn? (That is, why do agencies have difficulty devising and implementing corrective actions once lessons are identified?)

5. How do lessons-learned processes work?

6. How can they be improved?

We believe that by explicitly identifying persistent challenges, responders may be better attuned to these challenges and more able to address them in their planning and training processes. Likewise, by better understanding why these challenges remain unresolved, responders may be able to adapt their lessons-learned processes to better support behavioral change and improvement. To these ends, we have conducted a qualitative analysis of response organizations' perspectives on lessons and learning. The next section describes the context of emergency response learning. We then explain our investigative approach. Following that we present and discuss our findings about what lessons responders struggle with most and what learning approaches they use. We conclude with recommendations for improving these processes.

DISASTERS AND LEARNING

Disasters are devastating natural, accidental, or willful events that suddenly result in severe negative economic and social consequences for the populations they affect, often including physical injury, loss of life, property damage and loss, physical and emotional hardship, destruction of physical infrastructure, and failure of administrative and operational systems. Emergency managers and responders are responsible for intervening before and during such events, to minimize the harm disasters cause and to

restore order. The large scale, high complexity, profound urgency, and intense scrutiny that attend disasters provide a powerful motivation for responders to be good at response.

To address this challenge, responders use their experience to develop systematized strategies they can follow when the chaos of disaster erupts. At the same time, the infrequency with which disasters occur makes it hard for responders to test and improve their strategies, to ensure that they can be counted on to mitigate threats and hazards predictably and to resolve their consequences effectively. The appeal of learning from experience – both to avoid duplicating mistakes and to be able to repeat successes – is widely perceived, and many organizations across the emergency response disciplines have formal procedures for identifying, documenting, and disseminating lessons from incidents in hopes that they and others will be able to learn from past experience and improve future responses.

Various mechanisms for sharing experience have emerged. These mechanisms are generally termed "lessons-learned" processes, and include tools like in-progress reviews, after-action reviewing and reporting, "hotwashes," and various kinds of debriefings. While these processes vary, they have the common goal of sharing performance information in order to prevent the recurrence of adverse events and actions and to better contend with situations and problems that are likely to arise again. Most processes involve some version of three core components: 1. Evaluating an incident (through systematic analysis of what happened and why); 2. Identifying lessons (strengths to be sustained and weaknesses to be corrected); and 3. Learning (specifying and inculcating behavioral changes consistent with the lessons).

Examples of lessons-learned systems abound. One of the best known is the U.S. Army's After Action Review (AAR), a comprehensive reflective learning process developed in the 1970s.[1] Many emergency responders follow the AAR template to a greater or lesser extent, formally or informally. Post-incident reporting is a common practice whereby an agency or set of agencies documents what happened during a disaster or exercise. These reports usually include accounts of actions and results, as well as potential remedies to problems encountered. While these reports are often used internally by the agencies that generate them, they are often written in isolation by a single agency, rather than through a coherent inter-agency process. There are various collections of lessons that have been compiled for broader distribution. Prominent examples include the Wildland Fire Lessons Learned Center collection and the recently established Lessons Learned Information System (developed by the memorial Institute for the Prevention of Terrorism and sponsored by the Department of Homeland Security).

Despite these widespread activities, however, the term "lessons learned" is often a misnomer. Our experience suggests that purported lessons learned are not really *learned*; many problems and mistakes are repeated in subsequent events. It appears that while review of incidents and the identification of lessons are more readily accomplished, true learning is much more difficult. Reports and lessons are often ignored,[2] and even when they are not, lessons are too often isolated and perishable, rather than generalized and institutionalized.

METHODOLOGY

To determine whether or not our instinct is correct – that emergency response

organizations find it difficult to learn certain lessons – and to better understand why this is the case, we decided to conduct an exploratory analysis. We used three qualitative approaches in our investigation: interviews, a review of documents, and a focus group retreat. We began our study with a series of informal interviews with experienced emergency responders to confirm the face validity of our hypothesis that important lessons are repeatedly identified and to verify that this was a compelling concern for emergency responders. We then reviewed reports produced following incidents to discover and classify lessons that are identified repeatedly. We included reports from large incidents of all types that occurred within the past two decades. We excluded reports from military operations and from exercises. In many cases, individual organizations prepare their own reports, and so there are often several reports available for a given incident. In these cases, we focused on the reports prepared at the government level, rather than at the agency level, often by the department (or office) of emergency management, but sometimes by an independent analyst or commission. The reports we reviewed are listed in Appendix A.

Some reports were very general, identifying major issues and general lessons. Many, though, were very detailed and the descriptions and explanations provided were very particular to the incident at hand. Because we are interested in high-level, cross-cutting lessons, we confined our examination to lessons that were called out in an executive summary (if provided) or that were in some way highlighted as significant in the body of the report. Our review of these reports can best be characterized as systematic, but informal. That is, we did not apply formal coding schemes or use sophisticated textual analysis methods. While this would certainly be an interesting avenue for further analysis, our purpose was to determine whether significant lessons were common across reports.

Finally, we convened a focus group of eleven expert incident managers who could reflect on the persistent concerns that arise during major disasters. Most participants were chief-level officers. All were from major U.S. municipalities. All participants had significant senior-level management experience dealing with large scale incidents. Examples of incidents they had managed include: Hurricane Katrina (2005), the *Columbia* space shuttle crash (2003), the anthrax and ricin attacks in Washington, D.C. (2001), the September 11th attacks at both the World Trade Center and the Pentagon (2001), the crash of American Airlines Flight 587 (2001), the bombing of the Murrah Building in Oklahoma City (1995), the Northridge earthquake (1994), the World Trade Organization protests (1991), the Air Florida plane crash, as well as numerous other "civil" events such as presidential inaugurations, national political conventions, protests, major sports championships, Mardis Gras celebrations, and a multitude of natural disasters including wildfires, hurricanes, and tornados. Participants represented a range of emergency response disciplines including municipal and wildland firefighting, law enforcement, emergency medical services, urban search and rescue, and hazardous materials response. A list of the participants is provided in Appendix B.

During an intensive full-day retreat, we conducted a facilitated discussion to elicit the perspectives of these managers on our research questions. We had two primary objectives. First, we sought independent confirmation of the classes of lessons we discovered in our review of AAR's. To accomplish this we simply asked participants what major lessons seemed to come up repeatedly in their experience. Second, we wanted to elicit their beliefs about why these lessons were repeated rather than learned.

We asked them a series of open-ended questions about why lessons are hard to learn, how lessons are identified and reported, and what mechanisms are used to prompt learning. Three note-takers independently documented the discussion that ensued. Participants were also afforded the opportunity to provide additional commentary to clarify or expand points they wanted to make.

FINDINGS: WHAT LESSONS ARE IDENTIFIED REPEATEDLY?

To reiterate, we sought to be systematic in our analysis, but this remains an exploratory investigation – a first step in an area we hope to probe further in a more targeted way. The findings we report in this section were garnered both deductively (proceeding from loosely-specified hypotheses) and inductively (in that new and unexpected insights surfaced and added to our inquiry). Our findings are admittedly subject to the biases inherent in subjective, qualitative research. We hope to mitigate this threat by citing the perspectives of our participants directly, so that the reader can "hear" how these individuals characterized the issues at hand. Thus we report here our synthesized findings accompanied by illustrations from the discussions we held.

Our review of AAR's bears out our hypothesis that lessons are repeatedly identified. Despite the disparity of the reports we reviewed, we found a striking consistency in major categories of lessons identified. Table 1 shows important topics that were addressed in several prominent incidents. While it is certainly the case that each incident had its own unique challenges, it was common to see problems characterized in similar ways across several incidents. It is also true that the response to some incidents appeared to go well while the response to others went badly, so that certain lessons were stated as successes to be repeated in some cases but as problems to be corrected in others. A detailed list of the lessons identified in a selection of reports for significant recent incidents is available from the authors.

Lessons Learned Issues	Anthrax Attacks	Columbia Recovery	Columbine	Hurricane Katrina	Oklahoma City Bombing	SARS	September 11th	Sniper Investigation
Communications			●	●	●		●	●
Leadership	●	●	●	●	●	●	●	●
Logistics	●	●		●	●	●	●	
Mental Health					●		●	●
Planning	●	●	●	●	●	●	●	●
Public Relations	●	●	●	●	●	●	●	●
Operations		●	●	●	●	●	●	●
Resource Management	●	●	●	●	●	●	●	●
Training & Exercises	●	●	●	●	●		●	

Table 1: Common Categories of Lessons.
Correlation between After Action Reports from selected major incidents and significant issues addressed.

We gain added confidence in our hypothesis that these lessons recur from the responses of our focus group. The focus group participants were easily able to identify lessons that emerge regularly from incident responses. There was a very high level of consensus among participants about what these lessons are, and the lessons they identified are very consistent with those we identified from our AAR review. The lessons our incident managers singled out as important and recurring pertain to five main areas: command, communications, planning, resource management, and public relations.

Uncoordinated Leadership

We asked our incident commander focus group "what problems do you see on every incident?" Several incident commanders immediately replied: unclear, multiple, conflicting, uncooperative, and isolated command structures. Every head in the room nodded agreement. Large incidents demand that robust command and control structures emerge out of the initial chaos that inevitably ensues when disasters strike. Large incidents also involve a multitude of agencies, each of which must direct its own resources. As a result, agency- and/or function-specific command structures proliferate. Since each agency has legitimate missions, responsibilities, and jurisdiction, each uses its command and control process to take charge, in a legitimate attempt to solve the problems the agency is supposed to solve. Absent an overarching command structure to which all participants subscribe, however, the result is duplicative and conflicting efforts. As one responder put it, "People ask 'who's in charge?' The response is usually, 'Of what?'" In fact, a coherent joint command structure often fails to emerge; our focus group specifically cited weak implementation of the incident command system (ICS) and poor understanding of unified command. A fire chief with extensive experience at the Katrina response gave a telling example: "In New Orleans, you couldn't go two blocks without running into somebody's incident command post. But there was no coordination between them. Everyone assumes there'll be a graduation up to some larger structure, but nobody knows how to get to that." At the same time, by using the term "command and control," we do not mean to suggest that structures are unitary, rigid, or static. In fact, successful management requires collaboration, flexibility, and adaptability across multiple diverse actors. This cannot be achieved anarchically, however; it requires that managers employ common philosophies and conventions.

What accounts for command problems, for failure to collaborate? Our emergency response experts cited three main culprits. First, they said, agencies lack the commitment to coordinate with each other. At best, they are unaware of what other agencies are doing and do not try to find out. At worst, they are unwilling to cooperate. This stems from a lack of trust between agencies and a lack of understanding across disciplines. Moreover, agencies often find themselves in competition. Day-to-day they fight with each other for scarce budget resources. This battle worsens during a major disaster when resources become even scarcer. Second, responders told us that the primary mechanism for resolving resource-allocation struggles, the Emergency Operations Center (EOC), is often ineffective. The delegates sent to EOCs are usually liaisons who lack decision-making authority, aren't respected, and/or don't get along with each other. They do not focus on how to make decisions together. Worse, large incidents spawn multiple EOCs that tend to be political and parochial – they will not exchange representatives to facilitate coordination. As a result, "turf battles" rage and

distract incident managers from the real job at hand: mitigating the incident.

Finally, our experts told us, ICS is in common use, but it is not understood and implemented in a consistent manner. Generally, every discipline does their own form of ICS training and agencies train in isolation. Often this training is too simplistic to delve into the subtle skills of disciplined, team-based, decision making. Further, responders cannot be expected to learn the functions of incident management in the heat of an event. As one captain told us, "You can't grab 'regular' police officers and firefighters and take them away from handling the stuff they're handling to do incident management stuff. If they haven't already been training in logistics, it will take them a long time to figure it out, and they have other things to be worrying about." Yet, absent sound training, this is exactly what happens, with the needless result that recognized and well-developed incident management functions are carried out poorly. The reports cited in the introduction to this article bear out our focus group participants' claim that, as one manager put it, "Everyone agrees we need ICS, but we don't share one system."

Failed Communications

Our systems of command, control, and coordination are predicated on being able to communicate. As one expert told us, "For thirty years, we've said that communications is our biggest problem because it's a house of cards: When communications fails, the rest of the response fails." A major challenge of large disasters is that they destroy our physical infrastructure, including our communications equipment. The most recent example of this comes from Hurricane Katrina, which "destroyed an unprecedented portion of the core communications infrastructure throughout the Gulf Coast region… The complete devastation of the communications infrastructure left emergency responders and citizens without a reliable network across which they could coordinate."[3]

But communications isn't entirely (or even fundamentally) a technology problem. We know how to build robust equipment and systems; as one participant noted, "CNN never goes down." And even sophisticated interoperable capability exists. But our response professionals pointed to an unwillingness to agree to a shared system, a lack of commitment to operate using this system, and a lack of discipline to use it correctly. As one chief pointed out, "We dump millions into hardware, but don't think about systems. Hardware will do anything you want. You've got to get people to agree on how to function with it." In short, technology is only an enabler; communicating requires that people are willing to share information with each other. This is not to say there are no important technological weaknesses in our communications systems. In part, communications deficiencies stem from gaps in research and development, from resource constraints, and from problems making some technologies broadly available. As one responder lamented, "We can talk to a rover on Mars, but we can't talk to someone inside a building." Despite being aware of the limitations and fragility of the infrastructure, we continue to lack contingency plans for how to communicate when technology fails (or is destroyed).

Weak Planning

Gaps in emergency plans cause serious problems when disaster strikes. Witness the evacuation problems experienced in New Orleans: Thousands of people had no way to leave the city on their own and no place to go, leaving them stranded in the face of

Katrina. This problem was anticipated, yet the city's evacuation plan was woefully inadequate. While it mentioned evacuation, it lacked details about how evacuation would be conducted and who was responsible for the process, while some people who were assigned roles by the plan were unaware of their responsibilities. This is a prominent example, but not atypical of the response plans on which this nation relies. Plans are often simplistic and superficial, failing to provide enough detail to be actionable. Often plans cover the first hours or days of an incident, but do not consider long-duration responses or long-term recovery.

These gaps are a result of weaknesses in the planning process. The most fundamental problem to plague planning processes is a lack of commitment to plans across agencies and jurisdictions. While agencies may be at the table during the planning process, they may not buy in to the requirements needed to fully enact these plans. Alternatively, plans may be watered down to permit compromise, rather than requiring hard choices. Decisions about how work will get done are necessarily decisions about who has authority and who gets resources. These can be hard conflicts to resolve, and agencies often shirk making these hard choices when they are not perceived as immediately pressing. Worse, key agencies may be excluded from the planning process, even though the plan governs them or counts on their support. These problems are exacerbated by the fact that planning processes are typically infrequent, so plans become dated and do not incorporate lessons from recent events.

Ultimately these weaknesses go unnoticed because actual plans are not trained fully or exercised realistically. Plans are often developed by mid-level managers. Senior managers and political officials may have the plan on their shelves, but get no formal training on what is in it or how to use it. Similarly, plans are not disseminated to supervisors or training academies. When the time comes for implementation, those on the front lines don't know what the plan calls for.

Resource Constraints

Large-scale, long-duration incidents demand more resources – personnel, equipment, supplies, commodities, specialized capabilities – than any agency or government can keep on hand, so these resources must be obtained rapidly when a disaster occurs. This makes resource acquisition and management a major function of incident management. Unfortunately, while some materials are cached and pre-deployed, they are often inadequate to meet actual need. This means that resources must be obtained "real-time," but normal resource acquisition systems are too slow and are not designed to obtain large amounts of supplies rapidly. The capacity and flexibility of emergency requisition and purchasing procedures are uneven. Bid laws and ordering processes may be too cumbersome and constraining to permit responders to get what they need. Governments often lack standing contracts and agreements for specialized resources. Once materials are obtained, poor property-tracking systems leave response agencies vulnerable to public accountability problems and lawsuits.

Remedies to these problems do exist, but they are not broadly implemented. For example, there are one-stop-shop mechanisms available (such as those of the General Services Administration), but these are neither widely understood nor widely used, and the procedures involved must be pre-arranged. Mutual aid relationships can be an effective conduit for support, but these are often informal and are not centrally coordinated. As a result, a single mutual aid asset may be "counted" by several different

agencies as part of their resource bases. The wildland fire community uses a very effective nationwide resource ordering and deployment system, but this approach has not been replicated by other disciplines. Moreover, common terminology and standard resource typing are required for such a system to work; these do not yet exist across response disciplines.

Volunteers and donated resources present a particular challenge to incident management. Tracking systems for these resources are weak, and as a result many assets go underutilized. Many organizations have useful capabilities but do not know how to identify or connect to the incident management system, either because they do not understand ICS or because the command system is so fractured it is hard to navigate. Even emergency response agencies that do understand ICS often "self-dispatch" to the scene without coordinating their response. These agencies have important skills, but often deploy without the ability to support themselves with food, water, fuel, shelter, or communications. Also, it is hard to verify the credentials of personnel who show up to help; some are highly qualified, while others have no business being at an emergency scene. Yet there is no easy, standard way to confirm the background and affiliation of volunteers. Likewise, maintaining accountability and tracking volunteer status is equally difficult. As a result, well-meaning volunteers add a significant management burden to already over-taxed incident managers. As noted in Arlington County's report after 9/11, "Organizations, response units, and individuals proceeding on their own initiative directly to an incident site, without the knowledge and permission of the host jurisdiction and the Incident Commander, complicate the exercise of command, increase the risks faced by bona fide responders, and exacerbate the challenge of accountability."[4] On top of these problems, much of the material sent to the scene is not useful, but must still be managed – transported, stored, and disposed of. Agencies often lack plans for getting rid of stuff they receive but do not need.

Poor Public Relations

Responders told us they believe that the general public wants instructions about what to do, but that people may not receive or understand the directions government agencies give them. In part, responders say, this is because governments rely heavily on mainstream media. Many people don't pay attention to mainstream media, and therefore don't get the information governments want them to have. Even people who do get the information may not understand the message correctly, especially when the government gives short shrift to pre-incident public education. This problem is exacerbated in the heat of an incident – when agencies fail to use a common message, do not control the message carefully, the pressure to get information out quickly undermines accuracy, and rumors propagate unchecked.

Even when directions are clear, received, and understood, some people do not have the wherewithal to follow them. As our incident managers acknowledged, some people just do not have the will to do as they are told. In the incident managers' view, the public is generally complacent about preparedness. This is borne out by anecdotal evidence. For example, during the recent commemoration of the 1906 earthquake, National Public Radio reported, "Scientists agree that it's very likely another big earthquake will hit the San Francisco Bay area in the next thirty years, but…many people in the Bay Area still live in denial" (April 18, 2006). Interviews with a number of citizens illustrated their point. Few had serious plans or any supplies to sustain them in the event of a major

disaster. The lack of wherewithal or will on the part of the public presents a recurring challenge to governments that have not invested enough resources in emergency transportation and shelter.

FINDINGS: WHY DON'T WE LEARN?

These lessons relate to some of the most important and involved functions of incident management, so it is no surprise that problems are identified repeatedly in the areas of command, communications, planning, resource management, and public relations. Likewise, responders are most likely to notice concerns in these areas by dint of the effort expended on them during any incident. Moreover, large, complex incidents are inherently challenging to manage. Destructive and unpredictable, they impose extraordinary demands on the decision-making and service-delivery systems of the affected communities. Nevertheless, responders claim that many problems encountered repeatedly are solved anew each time, suggesting that it should be possible to inculcate improvements across time and agencies. It should be possible to solve at least some of these problems once and for all, rather than time and again. This section reports findings that illuminate the challenges to this proposition in five general areas: motivation, reporting, learning, exercising, and resources.

Motivation for Change

Learning is, at its core, a process of growth; thus a successful learning process requires a commitment to change.[5] Organizational change is notoriously difficult, but particular challenges attend change in the emergency response arena. One challenge is political traction. Individual citizens rarely see their emergency response systems in action. They generally assume the systems will work well when called upon. Moreover, citizens underestimate the likelihood that disaster will befall them. Yet citizens are confronted every day by other problems they want government to fix – failing schools, blighted communities, and high fuel prices. Politicians tend to respond to these more immediately pressing demands, deferring investments in emergency preparedness until a major event re-awakens public concern. As one incident commander put it, "Change decisions are driven by politics and scrutiny, not rational analysis." High-profile events and the media attention they garner generate opportunities to make changes because public fear prompts politicians to support improvements.

Scrutiny can free up resources for change, but the results can be perverse as well. Until Hurricane Katrina struck, the most momentous event in the public's memory was the 9/11 attack. On the basis of that incident, the president and Congress initiated a major new homeland security policy agenda, including one of the most significant government reorganizations in history. Many of the policies and programs promulgated under the auspices of homeland security are targeted at Weapons of Mass Destruction (WMD) and terrorism. This frustrates emergency responders who continue to struggle to maintain and upgrade their capacity to cope with a myriad of other (more common) threats and hazards. Our experts' frustration on this point was palpable. They find the WMD focus distracting. As one fire chief raged, "It's terrorism, terrorism, terrorism…and I can't use my resources for the things I know I'll face. So how many major non-terrorism incidents do we have to have before DHS get us resources for other things than WMD?" A police chief agreed: "Local agencies are having terrorism shoved

down their throats. They can hardly do basic tactical training because of all the mandates for certifications, much less terrorism training."

Even following a major event, it is hard to sustain a commitment to change long enough to accomplish it. After an incident, it takes time to conduct an analysis and identify lessons. Washington D.C. and the public have very short time horizons; neither waits for these reports to move ahead. The government tends to focus on fast (and inexpensive) solutions – quick wins they can point to before public attention wanes. This kind of nearsightedness is inconsistent with meaningful change. By the time reports come out, there is no will (nor funding) to implement changes. By then, leadership has either turned over or moved on to something else. One local manager told us "We thought we did a lot of work with our politicians after the last major incident. But they have better things to do. Five minutes after that incident is over, they're on to something else. There are a lot of gains to be made if they do well [managing a disaster], but an incident is a political flash in the pan for them."

Even in cases where important lessons do make it to the public agenda, the disparate emergency response community lacks a shared vision of what to do about those lessons. Response professionals see desired outcomes differently based on what agencies and disciplines they represent. Our focus group claims this problem has gotten harder since 9/11, because federal involvement in trying to solve problems is so much greater. The federal government has many resources to devote to policy and planning relative to local governments, who do not have much capacity. On the other hand, it is the locals who deliver services, are closest to the needs of the community, and best understand how to meet those needs, whereas federal agencies are removed from the exigencies of emergency response operations. As a result, federal and local agencies talk past each other. Even in cases where federal and local policymakers see problems the same way, federal ambition outstrips local capacity; federal agencies do extensive planning, but there are not enough local resources to meet the federal vision.

Another impediment to change is the episodic nature of significant events. Any given agency experiences incidents fairly infrequently, but looking at the nation as a whole, relevant events occur all the time. For the nation to improve response overall, the emergency response community has to be able to learn from all of these events. This calls for organizations to think of their experiences collectively, and be willing to learn from each other. But it can be difficult for agencies to perceive the experience of others as relevant to their own responsibilities and operations, and it can be hard to prioritize these lessons over the daily problems an agency confronts in its own jurisdiction. One chief told us, "There [are] no teeth in lessons from someone else's experience. We don't really learn from others unless we can really imagine ourselves in that other person's circumstance." Another explained the problem this way:

> We fail to recognize and apply the lessons on a daily basis. We kill firefighters over and over again the same way, report after report after report. We look for big lessons, but fail to identify the small ones and apply them in 'onesies' and 'twosies' every day. Why? We don't see the relevance, or think it won't happen here, or we're too parochial. We're tone-deaf to things that happen to other organizations. Distance in time and space makes this worse. As we get further from each other and the event gets further in the past, it is easy to ignore it. And, even if you accept that something needs to be done, how do you manage it with everything else that's coming at you as a priority every day? Small lessons just don't take priority.

Beyond this, it seems that pressure for change from within the discipline does not have the same force as external scrutiny. As we have said, public fear can motivate rapid behavioral change. An example that members of the focus group pointed to was the transformation in the active-shooter doctrine that resulted from the Columbine High School shooting. The protocol changed dramatically in eighteen months, and the change was universal – all S.W.A.T. teams in the country updated their procedures.

Why did such a sweeping change happen so fast on the basis of a single incident? There were three reasons. First, public scrutiny; every community had a school full of kids whose parents were afraid. Second, willingness to admit to an important lesson; the Columbine Police Department stood up and said, "We didn't handle this right." Third, rapid dissemination; the new protocol was sent to every department across the country through the law enforcement information network. Our focus group participants contrasted this example with the fact that it took five years and a lot of firefighter deaths to get Rapid Intervention Teams (RIT) established, even though many in the field knew they were necessary.

All of this suggests that thinking about learning and change in a single agency or discipline faces substantial barriers. Doing this work collectively is even harder, especially when long-standing animosity gets in the way. It is common for agencies to compete for attention and resources daily, and this only gets worse with big incidents. But one chief acknowledged that collaboration is a key enabler of learning. As he said, "If you're not alone in this game it's a lot easier. If you're learning alongside others who face the same problems and will be your partners in a major incident, then you're more likely to obtain broader, more persistent change because you change expectations across organizations."

Review and Reporting Process

Assuming that an agency is open to learning and change, the learning process can be thought of as beginning with the identification of lessons. This is typically accomplished through the publication of After Action Reports (AARs). Our response experts told us that while some reports are very comprehensive and useful, lessons reporting processes are, on the whole, ad hoc. There is no universally accepted approach to the development or content of reports. Moreover, there are often several reports that come out of any given incident. Sometimes joint reports are prepared, but more often agencies or disciplines write their own without consulting each other. These reports differ and even conflict, since perspectives and experiences (even from very reliable sources) vary dramatically, so that "sometimes you wonder if people were on the same incident." It is difficult for an agency seeking to learn from the reports to de-conflict them, since there is no independent validation mechanism to establish whether findings and lessons are "right."

Worse than conflicts and possible inaccuracies, concern about attribution and retribution is a severe constraint on candor in lessons reporting. It is politically dangerous for an agency or a leader to own up to mistakes and problems for fear that the leader or agency will be penalized. To contend with this, lessons are often reported in a much redacted way; as a result, the level of detail required to make a lesson meaningful and actionable is lost. Meaning is also diluted by the lack of a common terminology. The same functions are described using different terms in different disciplines and parts of the country. Or the same terms are used to describe different

things. This leads to a lack of understanding, or a false sense of understanding.

Another substantive problem is that the focus of reporting is unbalanced. AARs typically focus on what went *wrong*, but chiefs want to know what they can do that is *right*. Reports tend to detail things that didn't work, without necessarily proposing solutions. Incident managers seek a lessons-learned system that provides good answers, solutions, and best practices. They want to hear what *to* do, instead of what *not* to do. They would also like to hear about "near misses," things that almost went wrong and could go wrong again elsewhere without preventive action. This kind of reporting requires an additional analytical step; to produce reports that meet these needs, those preparing the reports need to understand not only what happened, but also why it happened and what corrective action would have improved the circumstances. Reports of this depth and quality are relatively rare. Beyond this, many opportunities to learn smaller but valuable lessons are foregone because formal reports are typically only generated for major events, not for small day-to-day incidents. These "less significant" lessons, if disseminated, offer important opportunities to make more manageable developmental changes in response procedures, but there is no mechanism by which these smaller lessons can be easily reported and widely shared.

The value of even well-crafted reports is often undermined because they are not distributed effectively. Most dissemination is informal, and as a result development and adoption of new practices is haphazard. Generally, responders must actively seek reports in order to obtain them. Lessons do get reported at conferences, but these discussions rarely trickle down to the front line. There is no trusted, accessible facility or institution that provides lessons learned information to first responders broadly, although some disciplines do have lessons repositories. (The Wildland Fire Lessons Learned Center and the Center for Army Lessons Learned are two prominent examples.) And there are some consolidated collections of reports that attempt to fill this need. (See, for example, the Memorial Institute for the Prevention of Terrorism's Lessons Learned Information Sharing web site.[6])

Learning and Teaching

Failure to learn is due, in part, to a lack of systems to identify and disseminate lessons. Even when lessons are identified, our response experts told us, most learning and change processes lack a formal, rigorous, systematic methodology. Simplistically, the lesson learning and change process iterates through the following steps: Identify the lesson → recognize the causal process → devise a new operational process → practice the new process → embed/institutionalize and sustain the new process.[7] It is apparent in practice that there are weaknesses at each of these steps.

Learning begins with an analysis to identify the causal process that underlies the lesson. Absent this, there can be no confidence that a remedy will work and this kind of analysis is rare. One manager explained, "We don't study lessons carefully enough and apply them in a serious way. We don't drill down into the details of what changes are really required to address lessons." In particular, our incident managers told us that agencies find it difficult to think in general terms to be able to see how lessons from one incident or discipline might apply to another. This dilemma is intensified by the fact that the emergency response disciplines writ large lack a common operating doctrine. Without common, accepted conventions against which to compare behavior, it is hard to spot deviations and inconsistencies that suggest the need for learning and change.

Moreover, agencies tend to consider individual incidents and particular lessons in isolation, rather than as systems or broad patterns of behavior. A chief put it this way: "We don't look enough at the relationships of components. Day to day, we focus too narrowly and short-term, so our problem-solving approach doesn't consider the whole *system*."

Following the analysis through which lessons are identified and appropriate remedies understood, practice is required to inculcate new behavior. Often the work of identifying relevant lessons and devising corrective actions makes the agency feel it now knows what to do. One responder admitted, "We spend a lot of time writing AAR's, which gives us the sense that we learned lessons, but the lessons are not consolidated into a training regimen, and so we don't actually learn them." Our focus group participants agreed that practice gets shortchanged. As a result, the link between the last two steps in the learning process seems especially tenuous. Agencies that do get to the point of practicing a new process are lulled into a false sense that they have now corrected the problem. But when another stressful event happens, it turns out this new process is not as firmly embedded as the agency thought. "We feel committed to new courses of action, but then they fall apart on exercises, much less incidents." A lack of practice means that processes have not been rehearsed well enough to work out details and problems, or to develop trust in the new process. Since responders do not really understand and trust the new process, they revert to their old familiar ways. These old habits seem "safer," even though past experience has shown they do not work. One chief described this pathology as follows: "Lessons represent dramatic changes that are hard to entrench. So we fail because we're not disciplined enough, and we fall back to old habits rather than sticking to what we learned."

This problem is rarely noticed until another event occurs because follow-up is inadequate. Our experts told us that feedback after implementing new practices is typically informal and passive; it comes from simply noticing improvement, rather than actively testing for it. One responder summed up the problem: "There are breaks throughout the cycle. Even if we could identify lessons, identify corrective actions, implement them, train them, and exercise them, how do we know if the changes solved the problem?" Lessons are not clearly linked to corrective actions, then to training objectives, then to performance metrics, so it is difficult for organizations to notice that they have not really learned until the next incident hits and they get surprised. As an Oklahoma City Chief told us about his experience after the Murrah Building bombing, "We'd been through a major incident, and when the next one was inbound, we thought we were ready, thought we'd learned and knew what to do. Then the incident hits and we have the same problems all over again. Turned out we didn't really learn what we thought we had." Responders from New Orleans echoed this sentiment: "We did Mardi Gras so well that Katrina felt like a sucker punch."

According to our focus group experts, fixing the weak links in the lessons learning cycle requires that response agencies have a deeper understanding of how to learn. But, they say, the learning process is not taught in our emergency response educational institutions. For example, the National Fire Academy (our premiere institution of learning in the fire service) doesn't teach learning science or systems thinking at any level of sophistication. Our emergency response agency leaders especially need this knowledge. One manager highlighted this need: "We don't know if we are even creating the mechanism appropriate to learning in our agencies."

Exercising

Perhaps the key mechanism for testing, practicing, refining, and inculcating new lessons-derived behaviors is exercising. Almost every AAR discusses the crucial role that training and exercising play in building capacity. Unfortunately, our AAR review and focus group betrayed several important weaknesses in the way disaster exercises are designed and executed.

One design problem is striking the right balance between the known and the unknown. On the one hand, it is very important to prepare for what is likely. But preparing for the events that will probably occur does not get responders ready for the unusual, unexpected, and unforeseen, and how to handle these kinds of circumstances. One chief asserted that "we don't use our imagination in preparedness," but also acknowledged the opposite problem: some exercise scenarios are so far-fetched that they are a waste of time. At the same time, responders, like citizens, would rather believe that the possible worst case just will not happen. This kind of denial stems in part from the fact that it is important for emergency responders to have confidence and courage in the face of extreme adversity. One incident manager explained: "The hardest thing is to train a firefighter or a cop to know that they're overwhelmed. They are trained to feel like they can handle it. It's a rude awakening to recognize your own mortality, but we've got to."

Another design problem is a lack of realism, not with respect to scenarios, but in terms of what is required of responders and incident managers. Exercise procedures are typically simplified, compared to how they would actually unfold in a real event, in order to meet the time and resource limitations of exercises. This masks complexity, however, and responders often fail to appreciate what it really takes to get work done; when reality hits, "the devil is in the details." One senior leader explained, "In planning and exercising, everything works nicely, but this doesn't happen in the real world." This lack of realism sometimes stems from the fact that exercises are rarely held without advance notice and tend to escalate progressively, rather than erupting suddenly on a broad scale. Sudden-onset incidents present a particular challenge for which responders need better preparation. One expert described his concern this way:

> As incidents escalate progressively in front of us, we build and add systems. We do this naturally. But what happens when the incident starts out big and requires a large system right out of the gate? We don't know how to handle instantaneously large, complex incidents. We go in thinking "I can handle this." We don't go in thinking "I'm overwhelmed from the get-go."

Finally, a major impediment to exercising is fear of failure – not in reality, but in the exercise. Our response experts told us that most exercises have a punitive tone. Exercise designers and evaluators have some "school solution" in mind that is never revealed to exercise participants. The participants do not understand in advance what the expectations are for success and the exercise objectives are unclear. As a result, participants make obscure decisions during the exercise, for which they are later criticized. This has occurred often enough that responders are reticent about participating in exercises. One senior manager explained the problem this way:

> We exercise wrong. People don't come to exercises because they're afraid they'll be tested, that they'll make mistakes, and that they'll be embarrassed. They make

> strange decisions that cause the exercise to veer off. We don't train people how to operate first and then test them afterwards. Instead, we throw them in blind, and then tear them apart afterwards. We just expect them to make the decision that we had anticipated and then criticize them when they don't.

This situation is not helped by the fact that exercises are often designed and delivered by contractors, whose interests may have more to do with business than with improving response performance in the field during a major incident. Our focus group participants fear that this punitive approach will only get worse if exercises become DHS's main tool for assessment and funding allocation.

There are also important imbalances in exercise goals and the content of exercise scenarios. Responders told us that the preoccupation with terrorism and WMD means that DHS mandates state and local governments to perform exercises they do not need, dealing with scenarios that are far down the list of likely events or do not focus on important capability gaps. In fact, a narrow focus on WMD is potentially damaging to our preparedness. There is only so much room on an agency's training schedule. If WMD displaces too much, there is not enough time to focus on training to address lessons the field has identified. Even making room for the most pressing lessons is already hard. Our experts assert that state and local governments need to identify their greatest threat and weakest capability and define their own relevant exercise needs.

Another common problem is that exercises have proliferated in light of events and studies highlighting weaknesses in preparedness. Not only are there too many exercises, there are too many goals for each one. As a result, locals are inundated with exercise requirements to the point that their participation is not productive. Our experts suggest fewer exercises with narrower and sharper objectives: "We are already exercised to death. More exercises is not the answer." Finally, exercises fail to target one of the most important levers of preparedness: regional relationships. Agencies either exercise in isolation with simulated interactions, or the interactions that are required by an exercise do not mimic those that would operate in a real disaster. As a result, agencies fail to derive perhaps the most important benefit of the exercise process: relationships with other agencies, jurisdictions, and disciplines.

Execution problems further undermine the value of exercises. A major problem is that many responders miss exercises, because they happen on a particular day and shift, and exercises of a particular type may happen only one time or once a year. So only some of the force gets the experience. Moreover, while the same agencies may participate together in several exercises, the participants vary from exercise to exercise. As a result, people have a "one-shot" experience and do not get a chance to learn from their mistakes and then try it again. Worse, uneven participation means that agencies miss the opportunity to build strong, trusting relationships. Finally, an important result of exercises is to expose deficiencies so that they can be examined and corrected, but fear of retribution or penalties impede honest reporting. Too often, public officials report wonderful successes and do not reveal problems. As a result, the public thinks everything is under control and has unrealistic expectations when a bad incident actually happens and agencies do not get the resources they need to correct problems.

Resource Constraints

Commitment to learning is wasted if resources are not available to support the process.

Unfortunately, funds available to sustain corrective action, training, and exercise programs are even leaner than those available for staff and equipment. One chief asked, "Even if we read every AAR, where do we get capacity to implement lessons in our organizations?" Part of the problem is that investments in basic capacity are not as marketable – as "sexy" – as equipment for combating terrorism. Furthermore, carefully conceived, sophisticated, progressive training and exercise programs are very expensive in time and dollars. Unlike the military, which spends a great deal of time training when they are not actually fighting, emergency responders have many other ancillary duties aside from responding to calls. Response agencies cannot pull personnel off the line or off these duties for training and exercises. And, our experts admitted, we shouldn't be investing resources in training and exercises unless we make the effort to improve our lessons-learning processes. "If you don't get the lessons right," they say, "you chase hollow solutions and throw money around without actually solving problems."

To synthesize our findings, we believe the fundamental challenge is that it takes long-term resource commitment and organizational discipline to solve recurring problems. Too often, however, political support is too transient as other, more visible, concerns divert resources from longer-term preparedness activities. Even in the emergency response domain, attention devoted to terrorism distracts from developing the basic capacity needed to respond to more common incidents. Agencies are easily distracted by their daily missions, as well. Because lessons from major incidents are not easily accessible, are not detailed enough to be useful, and their relevance is not immediately obvious, agencies are reticent about committing the time and effort needed to really understand, develop, and implement corrective actions that would improve their performance. Even if they do decide to adopt new procedures, inadequate practice prevents transitional changes from taking hold. Further, those changes most likely to become embedded are smaller internal adjustments, rather than broad culture changes that arise from a vision and doctrine shared across agencies, jurisdictions, and disciplines.

RECOMMENDATIONS

We asked our participants for ideas to improve our ability to learn the lessons of the past. Their ideas centered around three themes.

1. The need to radically improve the way we train and exercise.

2. The need for a comprehensive, nation-wide capability to gather and validate the information we learn from incidents, develop and vet corrective actions, and disseminate them to those who must inculcate the changes.

3. The need for incentives to institutionalize lessons-learning processes at all levels of government.

Training and Exercising

Across the board, our study participants felt the key to learning lessons is to improve the way we train and exercise. Most importantly, exercises must be recast as learning activities targeted at improving performance, not as punitive tests where failure is perceived as threatening an organization's ability to garner funding or maintain political

favor. This requires improvements in exercise planning. In particular, exercise planners should explicitly link the lessons a jurisdiction seeks to learn to a limited set of focused exercise objectives, rather than trying to accomplish numerous ill-defined goals. Our participants recommended that exercise planning should follow the military-style crawl → walk → run structure where participants first learn expectations about appropriate actions and decisions (crawl), then move slowly through a scenario taking the time to practice decision making (walk), and then pick up the pace and the challenges as they get more adept (run). This suggests that responders should engage in smaller, more frequent, narrowly tailored exercises with limited goals before they get to exercises on the scale of TOPOFF. An exercise program with this sophisticated, progressive structure is resource-intensive and will require federal support. DHS should reorient and enhance their exercise planning resources to help state and local agencies plan and execute exercises that fulfill these goals.

The participants offered advise for their own agencies as well, beginning with making training for large-scale events tougher. While the table-top exercises commonly employed provide valuable practice with strategic and tactical decision making, they are not realistic enough to test jurisdictions' abilities to coordinate resources and communicate with each other. We must find a way to introduce the chaos and common failures likely in a real event into state, regional, and local exercises. And local agencies need to find a way to inculcate practice with the protocols and behaviors suggested by lessons in daily activities. For example, jurisdictions that explicitly set up incident commands for every event they respond to – even the small ones – are better able to inculcate this way of operating as a habit responders will draw on during major incidents when it is especially necessary.

Finally, individual agencies also need to do a better job of adopting disciplined processes for reporting lessons and updating plans to reflect them, so that lessons, planning, training, and exercising can be better integrated. None of the lessons identified in this study as recurring are hazard-specific. They arise from incidents of all types. This suggests that even though disasters seem unique, solutions to them can be generalized. Most experienced incident managers will tell you that the best way to make a decision in an emergency is to make it well ahead of time, before an incident happens and before the specific nature of the problems that will arise is known. This suggests two things: first, that an all-hazards perspective is appropriate and should be emphasized, and second, that many of the issues that will arise from an incident of any type can be addressed in a rigorous planning process. To support lessons-focused planning, agencies must establish and follow a requirement to document events and lessons learned immediately post-operation, for small events as well as large incidents. Adopting a standard format for this process will make it easier for responders to follow this mandate. Agencies must also require that lessons learned (both theirs and other organizations') are consulted and considered as plans are revised. To assist this process, the incident managers in our study see an important role for the federal government in creating a national capability to identify and advocate lessons learned.

National Emergency Response Lessons Learned Institute

Learning lessons depends on the development of a robust analytical capability. Such a capability could be the core of a new national doctrinal institute or part of an existing federal academy or preparedness activity. Any of these arrangements would be a

significant undertaking, however, and would not succeed as simply an "additional duty" of an existing organization. Analysts who support this institution would need to be able to understand the information in AAR's, translate them into a common language, identify and resolve conflicting information or conclusions, develop the required changes in policy and procedure, vet or test those new concepts, and deliver them to the organizations who need them. This would require analysts with both expertise in learning science and in-depth knowledge and experience in the emergency response and incident management domains.

For this institute (whatever its configuration) to be effective, it must begin by promulgating a sound reporting system. Good reporting is demanding and resource-intensive; it requires clear criteria for what is to be reported, a standardized reporting process, a robust and secure data management capacity, and a user-friendly interface. A universal national reporting methodology would help response organizations understand what they should include in their reports so that they will be useful tools for learning and change. A common format would make it easier for agencies to understand each other's reports.

Once reports are submitted, the institute's analysts could work on understanding the lessons indicated in reports in order to consolidate findings and develop proposed procedural changes and alternatives, additions to doctrine, or new concepts of operations. Then, the institute should use sophisticated information technology to make their findings easily available across response disciplines. Tools such as databases with smart search engines, electronic update bulletins, and web-based training, should be employed so that responders could easily find information relevant to their missions, disciplines, service responsibilities, and hazard environments. Just creating a database will not be enough, however. It must be broadly recognized across response disciplines as a definitive, comprehensive, and valid information source. To ensure the ideas, information, and proposals generated by the institute are trusted by the response community, a peer review process to validate the lessons and ensure the proposed solutions are legal, workable, and effective is essential.

Also essential are activities to push important information out to users proactively and regularly through several modes and in a variety of forums. As examples, safety bulletins and time-sensitive alerts should be rapidly disseminated. A system akin to the National Law Enforcement Telecommunication System (NLETS) and other messaging systems currently used by police agencies could be effective. The institute should also have a regular publication and submit articles and columns in established emergency response trade journals. The institute should sponsor broad, multi-disciplinary, lessons-focused conferences. Finally, the institute should conduct senior leadership training forums that focus not only on lessons that need to be learned but on how to learn them.

A crucial concern when developing an effective lessons analysis institute is liability. For a lessons reporting and dissemination system to have integrity requires that those who report be protected from retribution. Absent this protection, reports cannot be specific enough to be useful. If lessons databases are fodder for lawsuits, jurisdiction attorneys may prohibit participation. The need for a high level of protection argues for enactment of such a system in legislation that assures immunity from Freedom of Information Act requests and restricts the use of reports in lawsuits, regulatory enforcement, or personnel actions. There are models for how a system like this could work. For example, the Aviation Safety Reporting System (ASRS) is a joint NASA-FAA

initiative that collects, analyzes, and responds to voluntarily submitted aviation safety incident reports in order to lessen the likelihood of aviation accidents. Pilots, air traffic controllers, flight attendants, mechanics, ground personnel, and others involved in aviation operations submit reports to the ASRS when they are involved in, or observe, an incident or situation in which aviation safety was compromised. All submissions are voluntary and reports sent to the ASRS are confidential. The FAA has committed not to use ASRS information against reporters in enforcement actions.[8] Another example that demonstrates how this might be developed for the emergency response community is the National Fire Fighter Near-Miss Reporting System, which is intended to be a voluntary, confidential, non-punitive, and secure reporting system targeted at improving firefighter safety by sharing the details of unintentional unsafe occurrences. It is currently funded by grants from the Department of Homeland Security's Firefighters Grant Program and the Fireman's Fund Insurance Company.[9]

Incentives

The incident commanders who participated in our study pointed out that discussions of lessons are moot unless they can be disseminated to the grass-roots level nationwide so that line responders can adopt them. They noted that it is important to recognize that people respond to incentives – that is, line troops will change their behavior to reap rewards or avoid punishment. Currently, fear of retribution drives responders away from participating in exercises or reporting their mistakes, for example. We need to develop incentives that cause regions and localities to support and promote lessons reporting, change, and learning. One obvious approach is to make federal and state funding contingent on developing and using lessons-learning systems. This kind of "carrot" can work. For instance, Fire Act and SAFER grants require that agencies participate in the National Fire Incident Reporting System for the grant year and three subsequent years. This is one possible model.

In order to achieve broad consistency, our participants argue that it is important to promote a regional commitment to identifying problems and adopting best practices. They believe that local agencies were "more likely to adopt and indoctrinate lessons if the people they work with every day across a region are doing the same thing." Identifying appropriate regions is not a trivial task, however. Who constitutes the "right" set of local collaborators depends on the characteristics of the prospective participant jurisdictions, the resources they have available, and the hazards they face. Successful regions cannot be imposed arbitrarily; they should be formed according to some commonality identified locally. This will be especially challenging when natural regions cross state lines. Regionalization could be enabled by enhancing (and in some cases fixing) existing regional processes and mechanisms (e.g. Local Emergency Planning Committees and State Authorizing Authorities). Regional response plans could be a prerequisite for receiving funds from a regionally-targeted preparedness grant program. A federally supported regional exercise program could also promote broader inter-jurisdictional work.

CONCLUSIONS

The fact that challenges to learning lessons persist, despite regular experience with

them, is a serious concern. In today's environment, where the emergency response mission space is expanding dramatically to include broader homeland security responsibilities, the ability to capitalize on experience and improve capacity is ever more important. But organizations cannot just be told to "change." Enduring change needs to address the structure, system, and culture of an organization so that patterns of behavior can be adjusted. Truly institutionalizing a new process requires long-term commitment. This is what makes learning processes especially vulnerable: there are too many short-term distracters. Other political priorities, sensational concerns like terrorism, workforce turnover, other concurrent organizational change efforts, and daily missions all conspire to derail organizational transition. As a practical matter, then, the main problem with lesson learning can be seen as a lack of will and commitment, rather than a lack of ability. If lessons learned become a priority for leaders – especially local leaders who will be called to manage disasters directly – then lessons learned have a better chance of becoming a priority for everybody. Moreover, this commitment needs to be vertical; federal agencies must also commit to identifying and learning the lessons that are relevant to them. As one responder put it, "You can fix all the wagons locally, but if the wheels fall off FEMA's wagon, the system fails."

An additional conclusion is that most big lessons are inter-agency lessons. Learning them requires learning within and across agencies. It is not enough for agencies to try to learn these kinds of lessons in isolation. Despite its profound advantages, federalism gets in our way: we have national, state, and local governments but few robust regional forums for decision-making. Our system lacks substantial support and incentives for regional (multi-state within the nation, or multi-local within and across states) activities and for broad integration across the response disciplines. Disasters are regional – they do not recognize jurisdictional boundaries or disciplinary parochialism. Our systems for learning from disasters must therefore span these barriers.

Another key observation is that, as one reviewer of this article pointed out to us, much of what after action reports focus on is tactical, operational, and retrospective in nature. Reports tend to offer relatively little insight into the more strategic dimensions of disasters, and do not tend to take a prospective view of what can be done to prevent them. Our purpose in this article has been to consider how well we learn from our experiences, with the contention that it is by learning from successes and mistakes that we can be better prepared to act when something else happens. Yet, we also believe that prevention is an important (and often ignored) goal. This suggests two things: first, those who prepare reports often forego the opportunity to comment on how to avoid problems altogether (rather than contending with consequences); and second, further research is warranted to understand learning in the context of prevention (as opposed to response).

Finally, from an academic perspective, focused research can improve our understanding of how to make lesson learning work well. Immediate research opportunities include more rigorous textual and content analysis of the AAR's to validate our suggestive findings, to identify causal processes (understanding of which may enhance learning), and to understand the differences in perspectives that emerge across all agencies participating in the same incident. Researchers should bring the learning science and social psychology literature to bear on developing approaches to effective learning tailored to the challenges of preparedness and emergency response. In short, helping organizations navigate the complexities of lessons learning should be

informed by the substantial academic literature that has developed around this issue. A brief synopsis of some key insights is included in Appendix C for reference.

The very real consequence of failing to learn lessons is loss of lives and property. In short, as one responder told us: "If we don't learn these lessons, people are going to die again, because we failed to fix the problems that killed people the last time." We should not belittle the magnitude of this challenge, however; problems recur because they are inherently very difficult to solve. If solutions were evident, emergency response professionals would have adopted them long ago. This should motivate agencies in all emergency response disciplines and at all levels of government to give serious attention to the goal of inculcating a culture of learning from past disasters to prevent future losses.

This paper is based on research sponsored by the Memorial Institute for the Prevention of Terrorism and the Department of Homeland Security Science and Technology Directorate's Emergency Preparedness and Response Portfolio. We are grateful to the incident managers who participated in this project, to Michelle Royal for her extensive research support, and to Tempril Moore for her administrative support.

Amy K. Donahue *is associate professor of Public Policy at the University of Connecticut. Her research focuses on the performance of emergency services agencies and citizen preferences for public safety. Since 2002, Dr. Donahue has served as a technical advisor to the Office and Department of Homeland Security, helping develop programs to meet the technology needs of emergency responders. From 2002-2004, Dr. Donahue served as senior advisor to the NASA administrator and she now sits on NASA's Aerospace Safety Advisory Panel. Dr. Donahue has many years of training and field experience as an emergency responder, including managing a 911 communications center, and working as a firefighter and medic. She served in the U.S. Army, rising to the rank of Captain. Dr. Donahue holds her Ph.D. in Public Administration and her M.P.A. from the Maxwell School of Citizenship and Public Affairs at Syracuse University. Her B.A. from Princeton University is in Geological and Geophysical Sciences.*

Robert V. Tuohy *is vice president for Strategic Planning at Hicks & Associates, Inc. where he focuses on homeland security policy and has led Project Responder for four years. Besides leading the development of Project Responder's National Technology Plan for Responding to Catastrophic Terrorism, he is also assisting the Department of Homeland Security in assessing emergency response preparedness and addressing the nation's Border & Transportation Security technology needs. Prior to joining Hicks & Associates, Mr. Tuohy served as the director of Science and Technology Plans & Programs in the Office of the Secretary of Defense where he was responsible for developing and coordinating the department's science and technology strategic planning and program assessment activities. Mr. Tuohy has a B.A. in Applied Behavioral Sciences from the National-Louis University, and an M.S. in Science and Technology Commercialization from the University of Texas at Austin.*

APPENDIX A: AFTER ACTION REPORTS REVIEWED.

Allan, Susan. 2002. "Anthrax – Local Response and Lessons Learned." Presentation to the NACCHO Annual Conference by the Health Director, Arlington, VA.

Arlington County. 2002. *Arlington County After Action Report On The Response To The September 11 Terrorist Attack On The Pentagon*. Prepared for Arlington County by Titan Systems Corporation under a grant from the Department of Justice, Office of Justice Programs, Office for Domestic Preparedness, under Contract Number GS10F0084K, Order Number 2001F_341.

Crupi, Robert S., Deborah S. Asnis, Christopher C. Lee, Thomas Santucci, Mark J. Marino, and Bruce J. Flanz. 2003. "Meeting the Challenge of Bioterrorism: Lessons Learned from West Nile Virus and Anthrax." *American Journal of Emergency Medicine* 21 (1): 77-79.

Ekard, Walt, W. Harold Tuck, Jr., and Deborah Steffen. 2003. *San Diego County After Action Report: Firestorms 2003*.

Federal Emergency Management Agency. 2003. *Columbia Recovery Mission Hotwash Report*.

Florida Governor's Disaster Planning and Response Review Committee. 1993. *Final Report*.

Gursky, Elin, Thomas V. Inglesby, and Tara O'Toole. 2003. "Anthrax 2001: Observations on the Medical and Public Health Response." *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science* 1(2): 97-110.

Herbert, W. Robert Chairman, Claire A. Collins, Member, Wm. B. Rowland, Jr. 2003. *An Assessment: Virginia's Response to Hurricane Isabel Submitted to The Honorable Mark R. Warner, Governor of Virginia*. Arlington, VA: System Planning Corporation.

Jenkins, Brian Michael and Frances Edwards-Winslow. 2003. *Saving City Lifelines: Lessons Learned in the 9-11 Terrorist Attacks*. San Jose State University: Mineta Transportation Institute.

Manzi, Catherine, Michael J. Powers, and Kristina Zetterlund. 2002. "Critical Information Flows in the Alfred P. Murrah Building Bombing: A Case Study." In *Terrorism Studies Series, Special Report 3* prepared for the Memorial Institute for the Prevention of Terrorism.

Memorial Institute for the Prevention of Terrorism. 2002. *Oklahoma City – Seven Years Later: Lessons for Other Communities*.

Murphy, Gerard P. and Chuck Wexler. 2004. *Managing a Multijurisdictional Case: Identifying the Lessons Learned from the Sniper Investigation*. Police Executive Research Forum for the Office of Justice Programs, U.S. Department of Justice.

National Aeronautics and Space Administration. 2003. "Interagency Jointness (Initial Lessons Learned from Columbia Shuttle Recovery Operations)." Draft summary from a Presentation to the NASA Advisory Council.

National Commission on Terrorist Attacks. 2004. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. New York: W. W. Norton & Company.

Oklahoma Department of Civil Emergency Management. 2003. *After Action Report: Alfred P. Murrah Federal Building Bombing, 19 April 1995 Oklahoma City, Oklahoma*. Department of Central Services Central Printing Division, Publications Clearinghouse of the Oklahoma Department of Libraries.

Oklahoma Department of Civil Emergency Management. 2005. *After Action Report: Alfred P.*

Murrah Federal Building Bombing.

Rothstein, Alcalde, Elster, Majumder, Palmer, Stone, and Hoffman. 2003. *Quarantine and Isolation: Lessons Learned from SARS*. Centers for Disease Control and Prevention.

Thompson, Kimberly M., Robert E. Armstrong, and Donald F. Thompson. 2005. *Bayes, Bugs, and Bioterrorists: Lessons Learned from the Anthrax Attacks*. National Defense University Center for Technology and National Security Policy.

United States Fire Administration . 1999. "Wanton Violence at Columbine High School" *Technical Report Series* USFA-TR-128.

United States Fire Administration, Federal Emergency Management Agency. 2004. *Responding to Incidents of National Consequence: Recommendations for America's Fire and Emergency Services Based on the Events of September 11, 2001, and Other Similar Incidents*. (FA-282-May 2004).

White House. 2006. *The Federal Response to Hurricane Katrina Lessons Learned*.

APPENDIX B: FOCUS GROUP PARTICIPANTS

Ed Bailor, Inspector, U.S. Capitol Police (Retired)

Steve Glynn, Chief of Special Operations, New Orleans Fire Department

Sam Gonzales, Chief of Police, Oklahoma City Police Department (Retired)

Jon Hansen, Assistant Chief, Oklahoma City Fire Department (Retired)

Bob Ingram, Chief-in-Charge of Haz-Mat Operations, New York City Fire Department

Kevin MacCurtain, Acting Fire Commissioner and Chief of Department, Boston Fire Department

Tom Miner, Program Manager, Washington Task Force One FEMA Urban Search and Rescue Team

Jon Olney, Battalion Chief, Kern County California Fire Department (Retired) and National Type 1 Incident Management Team Logistics Section Chief

Jim Schwarz, Chief, Arlington County Fire Department and Acting Director, Arlington County Office of Emergency Management

Mark Willow, Deputy Commander Policy and Planning, New Orleans Police Department

APPENDIX C: LITERATURE ON LEARNING AND CHANGE

This paper is about how emergency responders can more ably recognize flaws in past behavior and implement new behaviors that will result in better outcomes in the future. In short, we are concerned with learning and change. These are complex fields of theory and research. A brief review of some established insights from the literature is instructive.

Fiol and Lyles define learning as "the development of insights, knowledge, and associations between past actions, the effectiveness of those actions, and future actions."[10] Learning is multi-dimensional: it has cognitive, behavioral, and emotional components, each of which is susceptible to particular instructional or educational approaches.[11] The cognitive domain involves the attainment of knowledge and the development of intellectual skill. Rudimentary learning in this domain includes information acquisition and comprehension, while sophisticated learning involves synthesis and evaluation. The affective domain deals with emotional intelligence or the emergence of attitudes, values, and feelings associated with a particular phenomenon. Receiving and responding to these phenomena are at the lowest levels of learning, while organizing and internalizing values associated with the phenomena are at the highest levels. The behavioral domain involves learning that requires physical activity, ranging from simply observing an activity to adapting the skill to new purposes or origination of new action.

It is evident that learning is an individual-level activity – people use their brains to observe, think, reason, and develop new insights. But since the early 1970s it has been understood that learning also occurs at the collective level. That is, organizations can be considered to learn when they acquire, process, store, and distribute knowledge, understanding, techniques, and practices.[12] Organization theorists have long discussed how learning is shaped by the use of routines to guide behavior. Levitt and March summarize this body of thought as follows: Organizations depend on accepted routines (operational rules, procedures, and conventions that may be formal or informal). That is, they tend to follow habits believed to be appropriate to their circumstances, rather than selecting actions to achieve a particular result. These routines develop incrementally over time as a result of past experience, rather than consciously in anticipation of future conditions. Organizations adjust their routines based on successive comparison between outcome targets and the outcome levels they actually achieve. Thus, historical experience and established routine profoundly shape organizational learning.[13] From these insights, Levitt and March draw the important conclusion that "Organizations are seen as learning by encoding inferences from history into routines that guide behavior…The experiential lessons of history are captured by routines in a way that makes the lessons, but not the history, accessible to organizations and organizational members who have not themselves experienced the history."[14]

Organizational behavior (routines) change as errors develop in the organization's collective memory, as new experiences or the experiences of other organizations threaten the veracity of organizational beliefs about what is appropriate, and as the results of organizational activities diverge from desired or expected outcomes. As a result, organizations adjust their behavior. Meyer terms this adjustment "adaptation," and suggests that adaptation takes two forms: deviation-reducing (where adjustments are made based upon existing organizational assumptions) and deviation-amplifying (where adjustments use new causal relationships founded on revised assumptions).[15] To the extent that organizations must revise their assumptions, learning is fundamentally about changing culture, where an organization's culture is its system of shared values, perceptions of work, and perceptions of success.[16] To establish culture, assumptions are made and tested. When they are upheld, they become embedded ("frozen," in Lewin's classic conceptualization).[17] Culture change occurs when assumptions are challenged. Alternatives are proposed and tested, and if they are upheld repeatedly, adjustments may be made to adopt these alternatives. While this process of examining and revising assumptions is tacit, its effects are practical: for new organizational approaches to be upheld,

organization members must find them credible and witness short-term "wins." In short, lesson learning can require culture change.

An important question is what kind of change is warranted in light of what has been learned. An appreciation of the change process can help managers understand how to instigate and sustain it.[18] Ackerman distinguishes three types of change.[19] The simplest form of change – and a process that organizations commonly and comfortably use – is developmental change, which can be thought of as an incremental process of improvement and increasing sophistication. This form of change involves adjusting, enhancing, or correcting what already exists. It generally targets skills or methods that fall short of expectations or requirements. At the other extreme, the most difficult and disruptive kind of change is transformational change. This is radical change typically prompted by some shock to the organizational system that challenges the organization's assumptions about environmental demands, resulting in a period of chaos from which an entirely new culture or way of doing business emerges.

An intermediate form of change is transitional change, where an organization discards its old ways of accomplishing its work in favor of new processes.[20] Transitional change is planned, defined by movement to a known state. Typically an organization continues to use its existing process, but becomes increasingly dissatisfied with this process, either because it doesn't work well or it becomes known that something else works better. The organization develops a new process, which it then begins to "try out" in parallel with its old process. During this period of overlap, an organization works in its old process but may increasingly dip into the new process. As the organization gets comfortable and confident, it ultimately switches to the new process. But, if it doesn't have long or strong commitment, a difficult event may cause the organization to revert to its old habits.

What do these insights about learning and change suggest about why change in response to lessons identified from disasters is so hard? Developing a sustainable sense of commitment to a new process requires a persistent sense of urgency about change and improvement, but other political exigencies may overwhelm commitment to emergency response. Since disasters are infrequent, agencies do not have reason to adjust their operating assumptions, and lack continuous opportunities to test out and embed new processes. In effect, organizations will stick with their accepted routines, absent persistent challenges to their assumptions or feedback about their performance relative to desired outcomes. This problem is made harder when an agency is asked to consider a new process that comes, not out of its own experience, but from someone else's. Levitt and March tell us that organizations can capture the learning of other organizations through the transfer of encoded experience, though the mechanisms of diffusion (shared learning through a network) are even more complex than at the level of a single organization.[21] Thus we can anticipate that, absent an explicit strategy to learn and change, the emergence of improved behaviors may be slowed or even obstructed.

NOTES

[1] David A. Garvin, *Learning In Action, A Guide to Putting the Learning Organization to Work* (Boston: Harvard Business School Press, 2000): 106-116.

[2] Christopher Bellavita, "Olympic Security After Action reports and Why They Are Ignored," *After Action Reports* (2002).

[3] The White House, *The Federal Response to Hurricane Katrina Lessons Learned* (2006).

[4] *Arlington County After Action Report On The Response To 9 11 Terrorist Attack On The Pentagon* (2002), 12.

[5] The relationship between learning and change is well established in the organizational learning literature. We do not mean to suggest that learning and change are synonymous, but that the purpose of organizational learning in the context of disaster management is changed (presumably improved) behavior. As Argyris and Schön, note, " an important species of organizational learning consists in an organization's improvement of its task performance over time." Chris Argyris and Donald A. Schön, "What is an organization that it may learn?" In *Organizational Learning II: Theory, Method, and Practice* (Menlo Park, CA: Addison-Wesley Publishing Co, 1996), 4.

[6] See Memorial Institute for the Prevention of Terrorism's Lessons Learned Information Sharing web site at https://www.llis.dhs.gov

[7] These steps are synthesized from a larger discussion by Argyris and Schön, who explain, in part, that "Organizational learning occurs when individuals within an organization experience a problematic situation and inquire into it on the organization's behalf. They experience a surprising mismatch between expected and actual results of action and respond to that mismatch through a process of thought and further action that leads them to modify their images of organizations or their understandings of organizational phenomena and to restructure their activities so as to bring outcomes and expectations into line, thereby changing organizational theory-in-use. In order to become organizational, the learning that results from organizational inquiry must become embedded in the images of organization held in its' member's minds…" Ibid., 16.

[8] See http://asrs.arc.nasa.gov/main.htm for a full explanation of this system.

[9] See www.firefighternearmiss.com/home.do

[10] C. Marlene Fiol and Marjorie A. Lyles, "Organizational Learning," *Academy of Management Review* 10 (1985): 803-813.

[11] See, in particular, Edgar H. Schein, "How can organizations learn faster? The challenge of entering the green room," *Sloan Management Review* 34 (1993): 85-93; David R. Krathwol, Benjamin S. Bloom, and Bertram B. Masia, *Taxonomy of Educational Objectives Book 2: Affective Domain* (New York: Longman, 1999); Benjamin S. Bloom, ed., *Taxonomy of Educational Objectives, Handbooks I: Cognitive Domain* (Wokingham: Addison-Wesley, 1956).

[12] See, for example, Argyris and Schön and Lloyd Baird, John C. Henderson, and Stephanie Watts, "Learning from action: an analysis of the Center for Army Lessons Learned (CALL)," *Human Resource Management* 36 (1997): 385-396.

[13] Barbara Levitt and James G. March, "Organizational Learning," *Annual Review of Sociology* 14 (1988): 319-340.

[14] Ibid, p. 320.

[15] A. D. Meyer, "Adapting to environmental jolts" *Administrative Science Quarterly* 27 (1982): 515-537.

[16] Argyris and Schön; Also Edgar H. Schein, "Three cultures of management: the key to organizational learning," *Sloan Management Review* 38 (1996): 9-21.

[17] K. Lewin, *Field Theory in Social Science* (New York: Harper Row, 1951).

[18] J. P. Kotter, *Leading Change* (Boston, Massachusetts: Harvard Business School Press, 1996).

[19] Linda Ackerman, "Development, Transition, or Transformation: The Question of Change in Organizations," in *Organizational Development Classics*, eds. Donald Van Eynde, Judith Hoy, and Dixie Cody Van Eynde (San Francisco: Jossey-Bass, 1997): 45-58.

[20] Rosabeth Moss Kanter "The Change Masters," in *Organizational Transitions: Managing Complex Change*, eds. Richard Beckhard and Rubin T. Harris (Wokingham: Addison-Wesley, 1987). See also D. Nadler and M. Tushman, "Organizational framebending," *Academy of Management Executive* 3 (1989): 194-202.

[21] Levitt and March, "Organizational Learning."

Social Capital: Dealing With Community Emergencies

Russell R. Dynes

Recent events in the United States have generated considerable discussion about dealing with emergencies. Such discussion has produced congressional investigations and governmental reorganization while blaming victims for their own ineptness. Much of that discussion misses the point. Every community shows evidence of past problem solving and many of those problems were considered emergencies. Everywhere, people solve their problems within their own social and cultural context. Cities that experienced traumatic damage in World War II – London, Hamburg, Dresden, Hiroshima, and Tokyo – are still vibrant communities.[1] San Francisco recently celebrated the 100th anniversary of the 1906 earthquake. Some celebrated the city's continuity but others predicted a dangerous future. We easily recall the disasters but forget the continuity and creativity of these communities.

When new threats appear, they are usually seen as more deadly and more disorganizing than those that have come before. On the other hand, we often miss the effectiveness of individual communities in addressing these threats. In 1995, when the federal building in Oklahoma City was bombed by domestic terrorists, the city was home to a population of 450,000 and had fifteen hospitals. Within ninety seconds after the blast, emergency medical services had seven ambulances and two supervisory vehicles en route to the scene. The final report indicated that by 9:45 a.m., there were more medical personnel, drivers and people wanting to help than the site could handle. By 10:30 a.m. there were 442 people treated at various emergency rooms, eighty-three hospitalized and 243 treated by private physicians; all live victims, with perhaps two exceptions, had been removed from the damaged building. This effort – centering on a bomb-destroyed building – involved 167 deaths and 675 non-fatal injuries. The unanticipated emergency response from the community dealt with the immediate injuries in a little more than an hour.[2]

Of course, the central symbol of international terrorism in the United States was the collapse of the World Trade Towers in New York and the perhaps 3,000 deaths that resulted from the collapse. Often overlooked, however, is the fact that at the time of impact there were an estimated 17,400 occupants in those buildings and eighty-seven percent of them evacuated successfully. Most of the deaths were on the floors or above the floors where the planes hit. It is now determined that ninety-nine percent of those below the impact floors successfully evacuated.[3] This successful evacuation was not accomplished by conventional search and rescue groups; it was the result of people on site helping others and themselves to take protective action to get out of the towers and to a safe location. While the loss of property and life occurring on 9/11 is frequently recalled, the protective actions of the other "victims" in the building are often overlooked.

Much of the contemporary discussion about emergency planning assumes that community members "panic" and that strong authority is necessary. The vocabulary of "command and control" suggests chaos rather than citizen adaptability and creativity. Such assumptions can be questioned by the research evidence accumulated in recent years.[4] While we calculate damage to physical and human capital, we usually ignore the social capital available within communities to deal with emergencies. Social capital is our most significant resource in responding to damage caused by natural and other hazards, such as terrorism.

DIFFERENT KINDS OF CAPITAL

Insight into the ways in which communities respond to emergencies can be found by looking at the types of capital used to construct the human community. Most obvious is physical capital. We have tools and materials to build houses and streets, string wires or go wireless, build 110-story towers and create the material environment we experience every day. Also obvious is the necessary human capital. We build schools and colleges, as well as clinics and hospitals, to provide people with skills, knowledge, and health care. The concern for human capital is obvious. We want to improve it, not lose it, so we develop programs to improve test scores, increase stays in school, improve nutrition, and prevent diseases.

Most recently, attention has been given to another kind of capital: social capital. Social capital is not located in individual people, as is human capital, but rather is embedded in social relationships and networks between and among members of a community. These relationships can be used to guide collective action in emergency situations. In other words, even with losses to physical and human capital, social capital is less affected, can be quickly repaired, and provides an essential resource in accomplishing critical tasks.

The concept of social capital has been used in different ways. This discussion is based on the work of James Coleman, who identifies six different forms of social capital: obligations and expectations, information potential, norms and effective sanctions, authority relations, appropriable social organizations, and intentional organizations.[5]

Obligations and Expectations. Living within a community creates a network of obligations – to other family members and kin, to neighbors, workmates, other members of religious and social groups, and to unknown members of the community. Within this context, we develop trust that our obligations will be repaid when we need help. Over time, we build up many obligations that serve as an indication of the interconnectedness of our social world. These types of interconnectedness increase the resources available to all individuals involved in those relationships when a need presents itself. These obligations and expectations are rarely visible to "outsiders;" in fact, they may be difficult to articulate even for the people included in such networks. But they represent resources that will become available when the need is apparent and action is necessary.

Informational Potential. Information is important as the basis for action – what needs to be done. With sudden and unexpected changes, information can be obtained by using social relationships maintained for other purposes. While the

media has been given heightened importance in the modern world, individuals – by interacting with other informed members of the community – can increase their knowledge without having to obtain that information directly. In addition, while the media might provide "general" information, the specific implications for an individual have to be tailor-made. People talk to one another.

Norms and Effective Sanctions. The communication of a "declaration" of an emergency signals that self-interested behavior needs to be subjugated to the interests of the community. Norms defining what needs to be done and what should not be done organize action. They facilitate some actions and constrain others.

Authority Relations. When groups are organized to pursue specific goals, a leader is often chosen to make decisions and speak for that group. This leader has access to an extensive network of capital that amplifies the social capital of individual members. Such a leader can "volunteer" the network to engage in specific tasks. Volunteering is never an isolated act, but rather the action of some people involved in several other networks.

Appropriable Social Organizations. One outcome of social life is the creation of organizations for specific purposes. Most organizations, however, can be used for purposes other than those for which they were initially intended. A school intended to educate can be used as a first aid station, a shelter, or a coordination center, staffed by school personnel (including current students). A house of worship can be used in similar ways. Such reallocation of organizational effort provides flexibility to cope with unexpected problems. Routine activities can always be suspended for more urgent problems. This allows a community to reallocate its efforts and to utilize its physical and human capital in different ways.

Intentional Organizations. As human communities have added complexity, organizations engaged in recurrent activities of continuing value have emerged, each with its own history. Fire departments, police departments, emergency medical services, sanitation departments, traffic and parking have become routine and expected community services. Most recently, some political units (from local to national) have begun to think of emergency management as a routine community function. This has led to the development of specialized training and the emergence of a new occupation and career path. Such innovations point to another source of social capital now available to deal with emergencies.

The discussion here will focus on the community as the social system, within what are called developed societies, especially the United States. (Developing societies present a series of different issues, which will not be discussed here.) In part, the emphasis on developed societies is dictated by the scope of existing research available for analysis. Further, the focus will be on the response phase. It has become conventional to categorize disaster along a time spectrum – preparedness, response, recovery, and mitigation. The most difficult part of the spectrum to study is response, primarily because this phase is short and often unexpected. This makes response difficult for "planned" research. Much of the research on response has been opportunistic and lacking in the cumulative continuity necessary to develop generalizations. Also, some "response" research is done months and years after the

event, which raises questions about the nature of recall and, perhaps more importantly, misses the emergent qualities of the response.

The most systematic research on disaster response in the United States was initiated at the Disaster Research Center (DRC) in the late 1960s, where field teams were able to research a number of different communities.[6] Much of that research has been reported and published. In *Organized Behavior in Disaster*, conceptualizations from that fieldwork are recorded, in terms of the theoretical ideas that guided the research at that time.[7] Here, those materials are used as the basis for reconceptualization in terms of social capital. In addition, comments will be added from other studies of disaster response that illuminate this concept.

From the earlier research, the concept of emergence seems particularly important. The original DRC research design was predicated on a Time I/Time II comparison of changes in community structure. It soon became apparent that certain critically important elements in the response had no pre-response existence: the phenomenon called emergence. As Thomas Drabek suggests in a later summary article:

> What is it that makes an appearance? Within the literature, the two general categories of social phenomena have been described – behavior and expectations. In short, what emerges is a sequence of patterned behaviors – a social structure. These behaviors…may form relatively simple social systems.[8]

Here emergence is seen as the creation of new social capital. In many instances it emerges from existing social capital, but at other times it is "new" in that it is created to meet new problems created by the disaster. This view is contrary to most media accounts of disaster, which portray community structure as fragile and unable to deal with disaster problems, often implicitly suggesting that "survival" is dependent on external aid. As Coleman points out in an earlier and different context:

> It may seem paradoxical that problems create community organization, but such is nevertheless the case. A community without common problems, as many modern bedroom suburbs tend to be today, has little cause for community organization; neither does a community that has been largely subject to the administration of persons outside the community. When community problems subsequently arise, there is no latent structure of organization, no "fire brigade" that can become activated to meet the problem.
>
> A new town, a budding community, is much like a child; if it faces no problems, if it is not challenged, it cannot grow. Each problem successfully met leaves its residue of sentiments and organization; without these sentiments and organization, future problems could not be solved.[9]

It is the intent of this article to examine the research done on disaster response, primarily in the United States, in the context of the six dimensions of social capital identified by James Coleman. While the cited research was not initially guided by these concepts, there are sufficient descriptive materials to make realistic inferences.

OBLIGATIONS AND EXPECTATIONS

There are two rather dramatic changes regarding obligations that occur in the emergency period. Pre-disaster "normal" community functioning is oriented toward achieving many different goals relating to work, family, education, and leisure. A

disaster situation changes things rather dramatically since now community resources may not be sufficient to pursue all goals. Taking two illustrations, while health and medical issues are always important, the disaster situation increases their priority, centering on attention to disaster "victims." On the other hand, education (normally given a high priority), becomes less important; school buildings and school personnel can be utilized in ways related to caring for victims. In a sense, the pursuit of certain activities and obligations are reordered as to how they become relevant to disaster impact. This process can be referred to as the development of an emergency consensus.[10] It provides a new and distinct ordering of priorities, in contrast to the seemingly random and competitive activities of pre-disaster community life.

A second change can be seen as the expansion of the citizenship role. In "normal" times, the obligations of citizenship are quite modest, mostly centering around "housekeeping" norms relating to the maintenance of property, control of pets and children, making an appearance at neighborhood celebrations, exhibiting community pride at school athletic events, and participating in periodic elections. For some, the obligation may involve becoming a member of a volunteer fire department or providing goods and labor for events that support such communal activities. In most of cases, the costs of participation are minimal and even enjoyable. Disasters, however, create unknown problems (some even life threatening) and provide the opportunity for stronger identification with the community on the part of its residents. In effect, the obligations of citizenship are enhanced and the focus of activity is clarified. This provides guidance in sorting out the appropriate role behavior in response to the emergency.

Because individuals play multiple roles, they have multiple obligations and expectations. In sudden-impact situations, it is likely that the initial set of obligations is conditioned by a person's role at the time (the family role at home or the professional role at work). In some popular discussions of disaster, considerable interest has centered on the possibilities of role conflict: ways in which people were forced to choose between family-role obligations and disaster assistance. The general assumption has been that people abandoned their work roles, especially in emergency organizations. Research has shown that the image of roles as rigid and conflictual is less accurate than seeing roles as adaptive. Disaster situations often provide guidance on the importance of certain roles and obligations and highlight the lesser importance of other role obligations.[11]

Individuals in a disaster context have the potentiality of playing many different roles: family member, neighbor, worker, and for everyone within the community, the citizenship role.[12] For example, if a person engages in search and rescue activity, it might be done in terms of his or her specific role-obligation, or in relation to a more generic role as a "good" citizen. The felt obligation of the rescuer is, in large part, irrelevant to those rescued. Any disaster "victim" has a cadre of people who have an obligation to help; other family members, neighbors, workmates, or any other member of the impacted community.

The importance of obligations and expectations is reflected in search and rescue. During the first period after disaster impact, search and rescue efforts are carried on primarily by other "victims" in the area; they seek and extract victims and take them to where they can receive medical treatment.[13] When emergency medical personnel

arrive on the scene, they have to use the knowledge of neighbors to locate remaining victims and the members of the community continue to help in all phases of the rescue operation. Much of the rescue operation will be terminated when formal rescuers arrive. In the 1980 Italian earthquake, ninety-seven percent of the entrapped and injured victims evacuated and transported to medical care were rescued by bare hands and shovels, not heavy equipment.[14] This illustrates the importance of social networks. Of those who were trapped and living in single-person households, forty-six percent were rescued, as compared to sixty-one percent of people living in multiple households. People living in single households experienced a death rate 2.4 times higher than those living in households with one or more of the household present. Michael LeChat suggests that, given the usual delay in the arrival of external rescue teams and equipment, there is a need in earthquake-prone areas to educate local communities in rescue procedures, particularly since the longer a person is trapped, the higher the mortality rate.[15]

An excellent study of search and rescue following a gasoline explosion in Guadalajara, Mexico, in which victims had been buried alive and rescuers were near them, comments on these findings:

> People did not participate in the search and rescue efforts at random. Instead, their participation was a function of the strength of their preexisting social linkages and interdependencies with the victims and fellow rescuers. Their search and rescue efforts were part of a stream of ongoing social relations in which people participated, and from which their activities on behalf of their relatives, friends, acquaintances, or even strangers obtained meaning. The rescuers prioritized life; all human life was precious for them but the lives of those socially closest to them were deemed more important.
>
> The chances of people surviving the blast were directly proportional to the presence among the searchers of a person or persons who cared for the victim and who knew the victim's likely location at the time of the blast.[16]

Even the decision to seek medical help on the part of the victims is not necessarily obvious. A study of a sample of tornado victims in Edmonton, Alberta indicated that while 15.3 percent of the victims made that decision themselves, family and friends made 28.6 percent of the decisions. While 19.4 percent of the respondents did not know how the decision had been made, only 26.5 percent of the decisions were made by some 'official' source. In addition, about forty-five percent of the victims were provided transportation to medical attention by family, friends, and others; about the same percentage were transported by official means (ambulance, in the car, or by a casualty bus).[17]

In other contexts, family obligations continue to be important. "When people evacuate, they commonly do so as group members – most typically the group is a family unit. This means that evacuation planners at any level of government must explicitly recognize the social webbing and seek to design plans that complement it, rather than neutralize it."[18] When families evacuate, where do they go? Some studies show that up to eighty-five percent prefer to go to relatives and friends, rather than to public shelters.[19] That preference to stay with friends and relatives is reinforced by invitations offered by kin. A study of the May 1980 eruption of Mt. Saint Helens indicated that almost thirty-five percent of the evacuees were contacted first by someone at their evacuation destination.[20] All of this suggests that behavior during

the evacuation phase is prefigured by normal daily routines and action choices are guided by obligations that existed prior to the disaster situation.[21]

In a study of the 1985 Mexico City earthquake, which used a sample of the entire city population, ten percent of respondents indicated that they left their homes in the year after the earthquake; eighty-six percent went to relatives and another five percent went to friends. Of the people included in the study, 11.2 percent indicated they had temporarily sheltered relatives or friends in their own homes sometime during the year following the earthquake.[22]

While the previous examples emphasize the importance of family and neighborhood obligations, there is another source of obligations that are reflected in what we called earlier the expansion of the citizenship role. Residents feel obligated to participate in actions that will reduce the threat to other members of the community, even if family and other relatives have not been directly impacted by the disaster. A disaster occasion is characterized by a significant number of volunteers who become involved in a wide variety of assistance activity. Media depictions of volunteer activity often imply that the outpouring of volunteers is a consequence of "failure" on the part of organizations to mobilize regular employees. Or volunteers are seen as an interesting, but not very significant, source of help; at times, the reliance on volunteers is seen to support the argument for increased external help. In the Mexico City study cited above, there was an opportunity to ascertain the extent of volunteer activity and the ways in which volunteers had become involved. About ten percent of the sample indicated that they volunteered immediately after the earthquake. Such a percentage may seem small, but given the population base of Mexico City (one of the largest urban areas in the world) ten percent represents over 2,000,000 people – certainly a significant volunteer response.

Most of these volunteers either engaged in search and rescue or helped in the procurement and processing of supplies. Nearly half indicated that they had worked four days or longer, and almost eighteen percent had worked ten days or more. In terms of daily time commitment, forty-five percent said they had worked an average of nine hours a day. The volunteers were not just from the areas of the city immediately affected by the earthquake, but from all over the city; people who had no direct family or kin ties to the victims. This significant volunteer response occurred within the context of an estimated loss of less than two percent of the city's housing stock. Among our sample, only 5.5 percent suffered considerable damage to their housing, plus disruption of all utility services.

The volume of volunteers often creates a different type of problem for emergency managers. Instead of anticipating the lack of volunteers, a more important problem emerges: how to make the most effective use of the volunteers in realistic emergency activities. (Some community organizations will have extensive experience in utilizing volunteers in other situations.)

The importance of obligations and expectations as a form of social capital in disasters can be stated negatively in the following way. Socially isolated individuals are less likely to be rescued, seek medical help, take preventative action (such as evacuating), or receive assistance from others in the form of shelter. Conversely, existing social networks provide effective search and rescue in removing victims, helping them to seek medical attention, and providing transportation to medical help locations. The same social networks provide motivation and encouragement to

take preventative action, such as evacuation, by their willingness to provide temporary shelter as well as longer-term housing assistance. These same social networks are the channels that motivate volunteers to provide labor for important disaster-related tasks, which compensates for losses in physical capital.

INFORMATIONAL POTENTIAL

The role of informational potential as social capital can be identified in several different aspects of disaster behavior. Certainly, one of the universal observations regarding emergency situations is the increased need for information and the actual increase in information: The increase does not necessarily fit the need. When situations change, and a disaster is a classic case of a sudden change in reality, both individuals and social units need new information to orient their actions. For social units representing the community, this may mean "damage assessment" of what actually happened. Prior to impact, individuals may need to gather information for preventative action. Again, social networks provide the channels whereby individuals develop a perception of risk and are motivated to take some type of preventative action.

To illustrate this point, both warning and evacuation will be discussed in the context of information potential. There have been times, in certain situations, when "officials" have been reluctant to issue warnings based on their assumption that "people" would panic. In addition, evacuation has at times been discussed as a "failure of will" on the part of citizens who were trying to avoid some kind of threat. Fortunately, those assumptions are increasingly rare. But there are still troublesome assumptions, on the part of emergency managers, that the best way to warn people is to provide "official" public information through the media. This is based on the assumption that individuals will watch television or listen to the radio, hear the official warning, and consequently take the recommended action. Research-based descriptions of the warning process and effective evacuations underscore ways in which the "public information" imagery is likely to fail, however, and show how social capital is an important element in effective action.

In examining the research base on warning and response, Colleen Fitzpatrick and Dennis Mileti outlined the process in five different steps: hears, understands, believes, personalizes, and decides/responds.[23] Each of the stages is interactive and independent of individualistic mental stages. Other people help you "hear"; not everyone watches the media all the time. Others help you understand and believe; people still talk to one another. Others help personalize the message, pointing out that the general message actually applies to the current situation, and then assist in discussing appropriate action. Research has shown that if protective action is not taken, there is an effort to seek additional information. That is, the process is iterative. As Fitzpatrick and Mileti point out: "People respond to warnings through a social psychological process...which persons in an endangered public do and do not hear, understand, believe, personalize, and respond to emergency warnings is not the result of chance."[24]

Ronald Perry has developed a model to understand how people comply with an evacuation plan in a sample of three different disaster models. He underscores the importance of the social nature of the warning process, emphasizing the importance of warning-source credibility and the way in which warnings are confirmed by other

people; he also considers the content of warning messages. Perry notes, "The three events studied here represent comparable events in that each involved some forewarning and was characterized by definable speed of onset, duration of impact, and scope of impact." He adds, "the idea that the same model will predict evacuation behavior in connection with a flood, a volcanic eruption, and a hazardous materials incident, calls into question the popular strategy of classifying research on disaster events in terms of the type of event (e.g. Natural versus Manmade)."[25] Perry also includes family context in his model since evacuation is not individualistic; families evacuate as a group or, when missing members, only when those missing members are determined to be safe (although in Perry's samples, no family member was missing at the time of evacuation).

The importance of social networks for informational potential can best be appreciated when there are failures to take protective action. One such example, described by B.E. Aguirre, examined the conditions whereby the community of Saragosa, Texas was not provided tornado warnings. Saragosa, an unincorporated town in Southwest Texas, had a population of 428, and there were twenty-nine known deaths from the impact of the tornado. The community, comprised almost entirely of residents of Mexican-American descent, was part of a geographically large county. The description of the possible path of the tornado in warning messages was difficult to identify in familiar locational terms for those in the community. A major element in the warning's failure was that almost the entire community watched *Univision*, the national Spanish television network, which did not provide localized weather information. While some local radio stations did provide some warning messages, there were difficulties in making distinctions, in Spanish, between a tornado watch and a tornado warning, and the weather conditions immediately prior to the tornado provided few clues of the impending danger. As a result, the population of Saragosa did not receive the official warning messages, because their own social networks were isolated linguistically and geographically from the Anglo networks.

The importance of social networks as information potential is not undermined by the presence of several social networks within the same community. Certainly one of the key tasks of emergency managers is to understand the plurality of networks and how they might require different channels to convey important messages rather than assuming that a single media source will reach a mass audience and that all groups within the community will be part of that mass. This issue will become increasingly important since the 2000 census points to the growing diversity in the U.S. population; both television and radio address an expanding number of diverse audiences, reflecting distinctly different social networks. Returning to Fitzpatrick and Mileti's formulation of the warning process, if people do not hear, it is impossible for them to understand, believe, personalize, or decide and respond.

NORMS AND EFFECTIVE SANCTIONS

Effective norms constitute a powerful form of social capital. This form of social capital facilitates certain actions and constrains others. Allan Barton suggested a series of relationships between a disaster event and the emergence of altruistic behavior that continues to have considerable face validity.[26] Examples include: (1) The higher the proportion of victims and the average loss, the more communication

and knowledge there will be about the losses suffered by the victims; (2) When informal social connections are strong within a population, the sufferers are more likely to be more salient as a reference or identification group; (3) Social randomness of impact influences beliefs about the causes of the suffering; (4) The more communication and knowledge there are about the losses suffered by the victims, the more people will feel sympathetic towards them; (5) The greater the informal social connectedness of the community, the higher the percentage of members with opportunities to help victims; (6) The greater the proportion sympathetic to the victims, the more people will actually help the victims.

These propositions suggest that many disasters produce the optimum conditions for the development of altruistic norms. Disasters are relatively free of ideological disputes about cause, which tend to reduce channels of communication. If impact is sudden and creates socially random damage, this makes for greater saliency of sufferers as a reference group. All these conditions combine to create obligations to help and to emphasize helping as a community norm. The widespread perception of the community norm increases the actual behavior of helping.

In addition to the conditions that provide normative support for helping behavior, the development of an emergency consensus, mentioned earlier, provides a ranking of values and suggests that care for victims and the restoration of routine community services should assume high priority while education, leisure, and non-critical work efforts can be set aside until the higher priority goals are achieved. In addition to the effort directed toward high priority goals, there is a reduction in enforcement of what is seen as inappropriate norms for the situation. For example, conventional norms, which enforce appropriate work dress, are ignored; coats are replaced by jackets and dresses are replaced by slacks. In addition, certain conventional bureaucratic norms are abrogated – expenditures that require two signatures are made with one; meetings based on appointment are replaced by meetings based on need. In all of these actions, there is a greater informality and less attention to status. (In fact, one indication of the end of the emergency period is when such norms are re-sanctioned again.)

There are two situations that deserve mention here since they are, seemingly, attempts to sanction appropriate disaster behavior. First is the admonition frequently made by emergency officials in the media urging people not to panic. Second is the reassurance coming from various agencies that these agencies are doing "everything" to prevent looting. Both of these repetitive themes, accentuated during the emergency period, suggest that panic and looting are frequent and problematic in these situations. Research suggests otherwise, although this review centers on conclusions.

Panic describes a condition of acute fear coupled with flight. While extremely rare, it can occur when certain conditions are present – when people are aware of a specific threat to themselves, perceive they are entrapped, and are isolated from others – producing feelings of social isolation. These conditions are rarely found in disaster situations.[27] Many "victims" do have some anxiety and, in certain situations, flight may be a very appropriate response, especially if it is an evacuation.

It is obvious that the admonition not to panic is sometimes an expression of "macho" ideology. At other times it is an official message designed to encourage behavior an agency might desire, rather than letting individuals decide for

themselves, regardless of the "official" plan. In any case, such admonitions have little effect in curbing behavior that probably would not occur anyway. On the other hand, the belief that panic is a widespread response to disaster can be self-destructive if officials are reluctant to issue warnings and alerts because they fear citizens will panic if informed about potential risks. Otherwise, the ritual of reminding others not to panic is as effective as parental warnings to be good.

A second situation deals with the strong media focus on various efforts to prevent "looting." Such reports seem to suggest that looting is widespread and problematic during disasters. The concept of looting conjures visions of an invading army, but the evidence suggests that looting is a rare occurrence in natural disasters. Nevertheless, the image of disasters followed by the looting of property persists.[28] The primary explanation for this discontinuity – between popular conceptions and the absence of evidence for the behavior – centers on appropriate norms regarding the proper use of community resources after a disaster.

Property has reference *not* to any concrete thing or material object, but as a shared expectation about what can or cannot be done with respect to something. Property thus is a type of social relationship – a shared understanding about who can do what with the valued resources in a community. These understandings are widely shared and are embedded in legal norms indicating the appropriate use, control, and disposal of valued resources within the community. Those norms change radically in what are seen as wide-spread emergencies; the concern for property norms are reflected in the fear of looting. In this, the fear may be real but the behavior is infrequent or absent:

> In natural disasters, in American society at least, there quickly develops a consensus that all private property rights are temporarily suspended for the common good. In one way, all goods become community property and can be used as needed for the general welfare. Thus, warehouses can be broken into without the owner's permission to obtain generators necessary to keep hospitals functioning, and the act is seen as legitimate if undertaken for this purpose even though in a strict sense the participants might agree that it was technically an act of burglary. However, the parties involved, the local legal authorities and the general public in the area at the time of the emergency do not define such actions as looting and would react very negatively to attempts to impose such a definition.
>
> On the other hand, there is very powerful social pressure against the use of goods for purely personal use while major community emergency needs exist. In a way, the individual who uses anything for himself alone is seen as taking from the common store. The new norm as to property is that the affected group, as long as it has emergency needs, has priority.[29]

In both of these instances, panic and looting, there are convictions that such behaviors are both common and problematic. Perhaps the only way to resolve this contradiction is to see these convictions – that people behave badly in disaster – as symbolic sanctions for "appropriate" behavior in disaster, the recommended etiquette for unusual circumstances. Such concerns are symbolic reminders, not effective sanctions, aimed at preventing these behaviors from emerging. Again the preoccupation with preventing looting often leads to the allocation of security personnel to non-existent or trivial tasks. On the other hand, such an allocation is

likely to be successful since prevention is quite possible when the problems do not exist. Consequently, the concern for these issues following a disaster does not mean that they are, in fact, problematic, but rather that disaster provides the opportunity to celebrate the virtues of rational behavior and respect for property.

Finally, there are two special circumstances worthy of note. First, a number of researchers have commented on the development of "disaster subcultures." For example, Dennis Wenger has noted:

> ...in fully developed subcultures, the local community may not even perceive or define the impact of a disaster agent as being "disastrous." Some communities have institutionalized their mode of response to the point that they view such events as floods as simply nuisances or possibly even look forward to the flood period as a time of "carnival."[30]

Such subcultures arise in communities that have repetitive experiences with a particular agent so that the disaster occasion becomes a part of the annual calendar of community life. Norms-appropriate behaviors are already in place to cover the situation. Such subcultures tend to develop in communities where there is a considerable amount of instrumental knowledge based on previous experience.

A second circumstance has come about through the adoption of emergency planning by emergency organizations, especially those in the public domain with disaster responsibility. In this instance, there is the development of norms applicable to emergencies, which remain "latent" in non-emergency times. These may involve a responsibility to monitor particular hazards, planning for work force reporting and shift extension, and mechanisms for communicating organizational information to employees. Many of these latent emergency norms are simply extensions of routine organizational activities. The sanctions for violating these norms in an emergency context are already embodied in the reward and punishment system of the organization. So the emergency norms are unique only in the sense of the timing of their implementation, but they are based on the pre-disaster structure of these organizations. The transition does not lack continuity and is rooted in familiarity.

While disasters are frequently seen as situations of normative disorganization, in fact the social processes provide the conditions for priority and effectiveness. The development of the emergency consensus gives high priority to care for victims and the restoration of essential community services, and de-emphasizes other usual community activities so that human and material resources can be reallocated to the higher priority tasks. The conditions are such that altruistic norms are supported. Some of that support takes the form of rumors, moral tales, and stories that underscore appropriate behavior for the situation. The emphasis on, and spread of, emergency planning have provided guidance for appropriate behavior in emergency situations. All of these factors provide significant social capital for emergency situations.

AUTHORITY RELATIONS

To treat authority relations as a form of social capital in disaster response seems paradoxical, especially when a conventional view of disaster is seen as the prototype for social disorganization, primarily from the loss of authority. This conventional view of the loss of authority during disasters has been the rationale for public policy

arguments for the necessity to create "command and control" structures as a central feature of emergency management. On the other hand, in American society in particular, there has always been a popular skepticism of authority of all kinds and a particular distaste for those who claim authority without any social justification. This suggests that it is difficult to create authority for special situations. It also suggests that most forms of authority relations continue as social capital in disaster and that other forms can be modified, adapted, and transformed to fit the particular circumstances. Consequently, it is useful to talk about authority relations in the context of family and neighborhood, community organizations, and the community as a social unit.

Family Authority

As has been suggested in the discussion of obligations and expectations, family authority does not break down. In fact, family units continue to make allocative decisions as to how family resources are used. For example, in search and rescue efforts, family members can be "released" to assume certain disaster tasks while others take on additional family duties; a husband and wife may become involved in search and rescue efforts while assigning the oldest child or a grandparent to deal with childcare during that time. Too, it is quite common for certain emergency roles to be filled by families rather than individuals. A wife may have responsibilities to open and maintain a shelter operation for evacuees, while her husband and children deal with the shelter's day-to-day maintenance; children might be moved out of their bedrooms to house relatives whose houses have been damaged. These are all allocative decisions on how to use family resources, made within the usual family authority structure and through the usual decision processes. None of these decisions can be "mandated" by the community and none of them is planned or even anticipated, but they occur and constitute social capital. None of the activities violates or changes previous family authority.

Organizational Authority

Existing community organizations carry most of the burden of disaster response. The pattern of organizational involvement has been well documented by what has been observed in a variety of disaster occasions.

Figure I
Pattern of Organizational Involvement

STRUCTURE	TASKS	
	Regular	**Non-regular**
Old	Established Type I	Established Type III
New	Established Type II	Established Type IV

Four types of organization reflect two dimensions: structure and tasks. Some organizations perform the same tasks in disaster response that they normally do, but others take on new activities. Too, some organizations function with the same basic relationships among members during the disaster response than they had previously. In other cases, totally new structures emerge. By cross-tabulating the two dimensions (structure and tasks), four different types of groups can be identified.[31]

Using that typology, the implications for authority relations can be assumed. For example, established organizations (Type I) become involved in disaster response with the same authority relationships that existed prior to their response. A Type II organization continues with the same authority relations, but with expanded size and volunteers with previous involvement in the organization (and thus knowledge and some experience with the normative authority structure). Type III organizations have a pre-disaster existence, but extend their activity by dealing with realistic disaster tasks. This might be exemplified by a construction company that becomes involved in debris removal or a church group that takes over responsibility for a temporary feeding operation. While there are new tasks, the pre-disaster authority relationship continues. These personnel constitute a group rather than individual volunteers and, in their actions, they maintain their pre-disaster structure.

The only type not to have a pre-disaster history is the Emergent Organizations (Type IV). While there is a considerable literature on emergence, there has been little direct attention given to issues of authority relations.[32] One of the most complete descriptions of a work crew that emerged in the aftermath of a tornado is Louis Zurcher's discussion of the social psychological functions of ephemeral roles.[33] In that description, Zurcher emphasizes the development of a division of labor among the participants and the emergence of group solidarity. His description suggests that an emergent group that develops around an "immediate" need in the post-disaster environment is very task-related and the focus is on the division of labor necessary to accomplish those tasks. His description focuses on the process of differentiation; the work groups dissolved prior to any attempt to institutionalize and insure their continuity.

It is important to note that the different organizational patterns also have different combinations of social capital. For example, Type I organizations enter the emergency with homogeneous relationships – bonding relationships that strengthen the social capital that exits prior to the emergency period. On the other hand, Types II and III are usually a mixture of bonding and bridging relationships. Type IV emergent groups link parts of the community structure together, a linking necessary for the new tasks at hand. Such linking may have been unnecessary prior to the collective cooperative response. One consequence of this activity is to strengthen the identity of members of the community under crisis.

The pattern of involvement indicates that authority relations within organizations provide the social capital necessary for the overall emergency response. Authority relations do not have to be reworked in the disaster context and the return to the pre-disaster authority context is usually an easy transition. Emergent groups, however, constitute a newly-created form of social capital for dealing with newly-created and unanticipated problems. These groups tend to be task-oriented and the relationships within the groups tend to be based on an emergent division of labor in which authority relations are built on function rather than status.

Community Authority

There is a widespread perception, especially by the media, that there is confusion and disorganization within the community authority structure immediately after disaster impact. Such a perception more accurately describes a "natural" process whereby the community is able to achieve coordination of the many necessary tasks, some of which are new to previous community experience. In the early stages of disaster impact, there is uncertainty as to what has happened and urgency to act – to do something – on the part of community members. Mistakes may be made. Some organizations may allocate considerable resources to obvious, visible problems, which might not be central, given a more inclusive view. Some may over-mobilize, resulting from members wanting to do something. Others may find it confusing that volunteers are already doing tasks that organizations see as their exclusive province. Some organizations may find that they cannot "work" until another organization finishes its tasks. For example, one cannot transport injured people to the hospital until roads are cleared (what some call sequential interdependence).

These problems begin to be solved with efforts to coordinate community activity. Coordination is often a by-product of the search for information and leads to the development of a coordinating locus within the community (usually centered in the local government) that has come to terms with priorities.[34]

In this process of developing coordination, organizations with pre-disaster legitimacy continue. Police deal with social order and traffic. Fire departments deal with fire and other safety problems. Public Works departments deal with utilities and road problems. Hospitals and medical personnel deal with the injured. While some organizations might find themselves working with segments of the community for the first time in a new relationship, even emergent groups are an amalgam of pre-disaster authority relations rather than something completely novel.

In fact, the basis for the emergence of coordination of disaster tasks within the community is the pre-disaster authority structure. Thus, it is an important form of social capital. While some organizations may not be disaster relevant and may not be involved, others may play roles more important than those of their pre-disaster status. But the basic structures of the organizations that deal with the health and welfare of the community maintain their importance during the emergency period. In many ways, the priority of disaster-related tasks makes decision-making more rational. And one can argue that such decision-making is more effective than the diffuse and individualistic decision-making norm in the pre-disaster situation. In any case, the authority structures within families, within community organizations, and in the community as a whole generalize from their pre-disaster patterns and serve as the base for the community effort in the emergency period. They do not have to be changed or radically modified. Continuity is the dominant theme and familiarity is a consequence.

APPROPRIABLE SOCIAL ORGANIZATION

One result of a reordering of community priorities, as reflected in the emergency consensus, is that not only are certain tasks given high priority, but other activities are assigned low priority in the overall emergency needs. This means that many community members can be allocated disaster tasks, which can greatly increase the

available work force. Two forms of this reallocation of social capital are more common: Type II Expanding Organizations and Type III Extending Organizations (See Figure I).

Expanding organizations are designed to utilize volunteers who have previous contact with the organization. These individuals express their helping behavior through conventional social organization. They are members of or participants in an organization that has emergency responsibility in its charter and so has established plans that call for the addition of personnel to meet disaster needs. These organizations have a latent structure that is activated when emergencies occur. This latent emergency structure has, in its preplanning, already specified the necessary roles and relationships. When such a plan is activated, those who have positions in the emergency organization are notified by a call-up system or may report to assist simply by their recognition of the presence of conditions on which the plan is based.

Such a system for channeling helping behavior is characteristic of most traditional emergency organizations, such as police and fire departments, civil defense offices, Salvation Army units, public works organizations, and local Red Cross chapters. A police department may have an auxiliary police unit that is activated under certain conditions. The norms that guide helping behavior already exist within the pre-disaster organizational structure and, in addition, the volunteer is placed in preplanned social relationships. The volunteer fits into a rank structure within the auxiliary police unit, and the relation of the regular departmental authority structure has already been established. These structures allow for relatively efficient matching of personnel to tasks at hand in an emergency.

The second form of social capital reallocation, extending organizations, can best be described as a group of volunteers or members of an organization that has no specific emergency-related purpose. Such groups may, however, be concerned broadly with community service and so, when a disaster occurs, see disaster-related activities as a logical extension of their previous orientation. The individual group member does not volunteer; the organization does. The member's involvement is an extension of group membership. The behavior then follows pre-disaster patterns of social relationship, while new norms emerge, focusing group activity on new disaster-related tasks.

Examples of extending organizations include a scout troop mobilized by the scoutmaster to act as messengers for an emergency operation center; a church building used as a shelter and staffed by church members, or a parochial school staffed by the parent-teacher association; or a Veterans of Foreign Wars post that assumes responsibility for feeding disaster workers. In all these instances, considerable personnel can be mobilized quickly and channeled toward tasks created by the emergency. In addition to personnel, such groups and organizations have at their command many other types of resources – buildings, supplies, money, and information.

It is important to emphasize that the behavior of the two types of volunteers described above follows lines of already-established social relationships. These are not spontaneous, random acts of generosity on the part of isolated individuals; they are extensions of pre-disaster relationships.

INTENTIONAL SOCIAL ORGANIZATION

One can find, in the historic record, specific occasions when central governments have been involved in disaster situations, often with immediate relief. Most of that involvement has been on an *ad hoc* basis; when the immediate tasks were finished so was the governmental responsibility. In that context, the Lisbon earthquake of 1755 can be identified as the first modern disaster because of the emergency responsibilities initiated by the early patterns of a central government.[35] That has changed. E.L. Quarantelli, using the broader term of civil protection, suggests:

> As we enter the 21st century, civil protection has finally become explicitly accepted as a major governmental responsibility in practically every country in the world. At the national level, usually the relevant activity is quartered in a formal governmental agency, very close to but relatively rarely at the highest level such as a cabinet office.[36]

In the United States, a bifurcated system developed whereby national security issues were the concern of a national civil defense system, but local offices of civil defense were primarily concerned with local disasters. In a study of local civil defense in the 1960s by the Disaster Research Center, the following conclusions were noted:

> 1. The scope of disaster planning was broadened to include a wider range of disaster agents... 2. There was a decline in the assumption that preparation for a nuclear attack was sufficient planning for all types of disaster contingencies... 3. There was a shift in focus of disaster planning from the emphasis on security of the nation to the concern with the viability of the local community.[37]

The DRC report went on to say that in the 1970s, the local community civil defense offices varied considerably in the scope of the hazards with which they were concerned:

> Some are completely focused on planning and the associated task of dealing with nuclear attack. Others are primarily concerned with natural disaster hazards. Many are concerned with both but the degree of emphasis on one or the other will vary. A smaller number show a range of concern with a wide range of hazards – man-made, nuclear, natural disaster, etc.[38]

During the '60s and '70s new concepts emerged. There was considerable discussion of "dual use" – the idea that facilities could be used for both national security and local disaster problems. There was the notion that the focus should be on all hazards within the community and the idea of "comprehensive emergency management" (CEM) began to be seen as an increasingly important function of local government. In some states, divisions of emergency management were created. And, in 1979, federal agencies with disaster responsibility were combined and reorganized into a Federal Emergency Management Agency.[39]

The development of FEMA into a functioning emergency management organization took a long time. Its development as a federal/state partnership was enhanced by pressures on the agency from states where major disasters occurred. In addition, concern for traditional nuclear and civil defense issues receded. During the first Clinton administration, a former emergency management director from the president's home state began to restructure FEMA to deal with the full range of

policy concerns – from mitigation of hazards to disaster recovery. These concerns were severely truncated with the terrorist attack in New York on Sept. 11, 2001, a new presidency, and the incorporation of FEMA into a large new agency called the Department of Homeland Security (DHS).

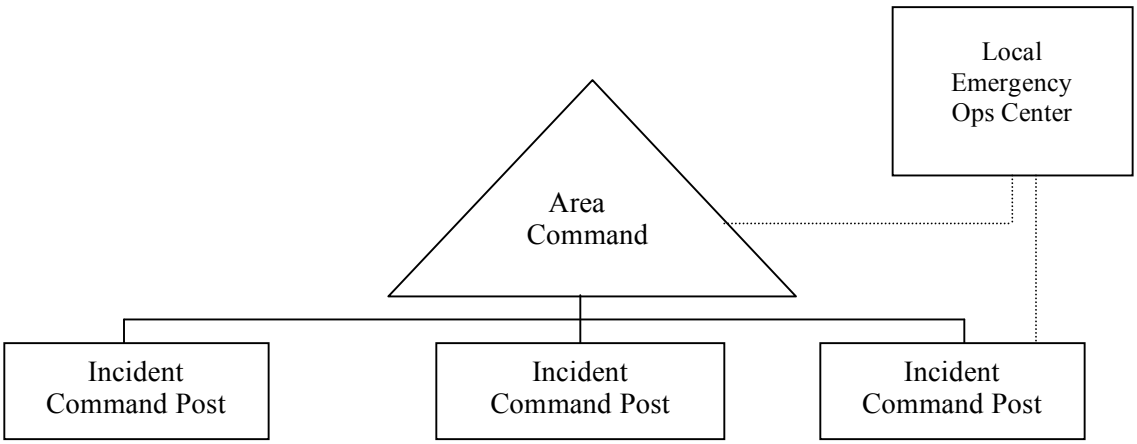
In general, this reorganization was made with the rationale of strengthening national security and addressing the threat of terrorism. In this transition, many of the assumptions coming out of World War II and the Cold War were revived and re-institutionalized. The necessity for homeland security seemed to be predicated on the weakness of individual citizens and the fragility of our social structure, requiring the government to enhance its ability to "command and control." The necessity of command and control has been revived and in general is based on a set of assumptions about what happens in emergencies, especially those caused by terrorist attacks. Specifically, the command and control approach:

1. Assumes social chaos and dramatic disjunctures during the emergency.
2. Assumes the reduced capacity of individuals and social structure to cope.
3. Creates artificial social structures to deal with that reduced capacity.
4. Expresses a deep distrust of individuals and structures to make intelligent decisions in emergencies.
5. Places responsibility in a top-down authority structure to make the right decisions and to communicate those "right" decisions in official information to insure action.
6. Creates a closed system intended to overcome the inherent weakness of "civil" society to deal with important emergencies.

The vocabulary of "command and control" is reflected in the issuance of a national response plan in December 2004 in which, in describing the proposed organization at the local level, "command post" terms are specified.

Figure 2

Organizational Structure



The national structure for incident management establishes a clear progression of coordination and communication from the local level to regional and national headquarters level. As illustrated in Figure 2, the local incident command structures (namely the ICP(s) and Area Command) are responsible for directing on-scene emergency management and maintaining command and control of on-scene incident operations.[40]

Alternative Assumptions

The first test of this "reorganization" in the United States came with Hurricane Katrina and was not reassuring. Perhaps the catastrophic scope of Katrina was not a fair test.[41] On the other hand, it prompted every legislative body, every political unit, and every media outlet to offer criticism, and some of the suggestions were relevant. Such criticisms have reenergized the move toward standardization, bureaucratization, and militarization of emergencies in modern democratic societies. This movement will continue to inhibit the effectiveness of social capital and to maximize the ignorance of authorities regarding the dynamics of the resources of local communities. These issues will continue to be problematic.

A much more realistic set of assumptions for emergency planning should center on "problem-solving" rather than command and control:

1. Emergencies may create some degree of confusion and disorganization at the level of routine organizational patterns, but to describe that as "social chaos" is incorrect.
2. Emergencies do not reduce the capacity of individuals and social structures to cope. They may present new and unexpected problems to solve.
3. Existing social structure is the most effective way to solve those problems. To create an artificial emergency-specific authority structure is neither possible nor effective.
4. Planning efforts should be built around the capacity of social units to make rational and informed decisions. These social units need to be seen as resources for problem solving, rather than as the problem themselves.
5. An emergency, by its very nature, is characterized by decentralized and pluralistic decision-making, so autonomy rather than the centralization of authority of decision-making should be valued.
6. An open system could be created in which the premium is placed on flexibility and initiative among the various social units, whose efforts are coordinated. The goals of efforts should be oriented toward problem solving, rather than avoiding chaos.

Kathleen Tierney observed that the response to the September 11th terrorist attack was so effective because it was flexible:

> The lesson here is that the response to the September 11th tragedy was so effective because it was *not* centrally directed and controlled. Indeed, it was flexible, adaptive and focused on handling problems as they emerged. It was a response that initially involved mainly those who were present in the

> immediate area where the attacks occurred and then later merged the efforts of officially designated disaster response agencies with those of newly formed groups as well as literally thousands of other organized entities that had not been included in prior emergency planning and that were not subject to any central authority.[42]

An alternative model for emergency response, based on the utilization of social capital, would be to use what exists and to capitalize on the characteristics that emerge during the crisis, rather than to create an artificial set of norms and structures. The continuity and persistence of behavior and structure that characterize the notion of social capital are evidenced in the following ways:

- Rather than interpreting emergencies as a direct break in experience, individuals tend to normalize threat, to define situations as normal, and to continue habitual patterns of behavior.
- Rather than exhibiting irrational and abnormal manifestations of behavior, individuals exhibit traditional role behavior and maintain occupational and familial obligations. Irrational and anti-social behaviors do not, in aggregate, increase (in fact, they probably decrease).
- Traditional social structures such as families maintain their viability and can be utilized to assume additional emergency responsibilities. For example, there is good evidence that almost all search and rescue activities are done by kin and neighborhood groups. In addition, there is evidence that warning messages are mediated through traditional social structures, rather than through impersonal media. There is also evidence that kin and neighborhood groups provide mass shelter for a large majority of affected populations and that planned mass shelter is useful only for a small segment of the population.
- Rational social structures such as community organizations maintain their viability and can be utilized to assume additional emergency responsibilities. For example, traditional health care institutions carry out almost all emergency medical care. Health care offered by first-aid stations or by hastily-constructed emergency facilities tends to be ignored and rejected.
- The way people define the situation and determine appropriate behaviors requires heightened, rather than restricted, communication. The command-control model places great faith on "correct" information, officially decreed. What are officially defined as rumors to be controlled are actually part of the definitional process. Thus, messages and channels of communication need to be increased rather than restricted.
- Rather than seeing self-initiated helping action as disruptive because such actions were not planned, it is more appropriate to see planned action as supplemental to self-initiated actions.
- Rather than attempting to centralize authority, it is more appropriate to structure a coordination model. The fact that emergencies have implications for many different segments of social life, each with their own pre-existing patterns of authority and the necessity for simultaneous action and autonomous decision

making, indicates it is impossible to create a centralized authority system (that it is probably unnecessary). The centralization of authority is usually predicated on the image of disintegration of social life. The evidence points to a viability of behavior and the adaptability of traditional structures, suggesting that authority is more of a problem in the minds of planners than an actual problem of life under emergency conditions. Planning should focus on coordination and the development of communications, rather than the creation of authority.

SPECIFIC SUGGESTIONS FOR ENHANCING SOCIAL CAPITAL

The basic assumption relating to social capital is that the local social system is the logical and viable base for all stages of emergency action. Certain specific courses of action can be suggested as a guide to policy:

1. Utilize a variety of mechanisms to increase community identification and collective responsibility. Enlist religious and other civic organizations to build disaster responsibility into routine messages about moral and civic responsibility. In particular, there is a need to remind the community that the greater the disaster, the more the community will have to depend on its own resources. Disaster memorials, anniversaries, and other civic occasions provide such opportunities.
2. Involve civic organizations in planning activities. Develop an inventory of and knowledge about community resources, both people and materials. Encourage organizations to develop certain useful disaster skills. For example, groups with physical locations, such as churches, schools, and some civic organizations, might develop skills in running mass feeding operations, shelters, information centers, etc. Local contractors might be encouraged to have meetings discussing the latest information on search and rescue in high-rise building collapses. Certain community skills such as knowledge of first aid might be encouraged as an important attribute of civic responsibility. More specific guidelines should be utilized for those community members engaged in disaster planning.
3. Utilize existing habit patterns as the basis for emergency action. To do this effectively, knowledge of the patterns of social life and their routines is essential. For example, in making plans for evacuation, it is best to utilize usual patterns, e.g. easily-designated and commonly-traveled routes.
4. Utilize existing social units, rather than create new *ad hoc* ones. If families are the major point of resource allocation within the community, utilize that system. Much of the thought in American society is individualistic; much of the activity in emergency situations is family-oriented. Organizations running shelters should think in terms of family units, not collections of individuals. The same thinking should characterize evacuation plans. In addition, much governmental assistance is directed toward individual applicants. To modify that suggests radical change, which is unlikely, but there needs to be a constant reminder that the "people" come in social units and need to be accommodated that way.

5. Utilize the existing authority structure, rather than create new ones. The speed with which decisions are made can be increased more easily by the use of a traditional structure than by the creation of a new one. The establishment of authority, which involves not only power but the acceptance of that power, takes time and is not easily or quickly reversed. It is better for outsiders to supplement local leadership than to assume locals are incompetent and incapable or outsiders are wise and competent.
6. Utilize existing channels of communication and increase them, rather than restrict and narrow them to "official messages." Information about potential risk, potential threat, and potential preventative action are not disorganizing; the lack of information, in the quest for certainty, may be. Any effective emergency plan is based on the autonomous and independent decisions of many to take appropriate action. These actions are more effective when communication is enhanced than restricted. Remember that people talk to one another, so these interpersonal channels should be used in addition to the mass media. Citizens are at work or school, engaged in many different collective activities and are not attached to the mass media. Remember that members of minority and immigrant communities may not access the same communication networks that the "official" community utilizes. Some citizens may be socially isolated because of disabilities, age, illness, and geographical location. Attempts to reach these people can also utilize conventional methods of social capital.
7. Since it is difficult for citizens or politicians to maintain interest in activities concerned with local risks, at least a minimum level of concern should be maintained by institutionalizing support for emergency management functions within local government. Encouragement should continue for training activities leading to the professionalization of the emergency manager. This task may be best supported at a national level. Collectively, training efforts should become an integral part of municipal services, which would require only a small part of the cost of current emergency services. This would mean the creation and cultivation of citizen lobbying for the initiation and continuation of such services, making them as routine as the functions of the police, fire, ambulance, and other emergency services.
8. The aim of emergency planning is to move back to the "normal" as quickly as possible after a disaster. This means the restoration of commerce, the reopening of schools, and the reinstitution of usual community patterns. Inconvenience is more easily adapted to than absence. And the therapeutic process, both for individuals and communities, is enhanced by the reestablishment of habitual actions.
9. The recovery stage should not be seen as the opportunity for massive (and directed) social change. Nor should possible mitigation opportunities during the recovery be implemented so as to drastically alter the traditional social structure of the community. This does not imply that

> there are no opportunities for mitigation during the recovery period; it suggests these opportunities be approached with humility rather than enthusiasm. Mitigation efforts can be effective if adapted to local community practices.

LOOKING BACK AND FORTH

This article began as an effort to examine the utility of the concept of social capital when applied to the existing research findings relating to disaster response. This concept has the advantage of moving away from a current preoccupation with hazards as a cause of, and mitigation as a solution to, disasters. It has the advantage of shifting attention away from making the environment sustainable and looking at how social systems can function in any environment. The concept of social capital has the advantage of seeing social systems as active resources, not passive victims, shifting the focus away from human vulnerability toward an emphasis on human capability. It has the advantage of identifying the creation of social resources in emergency situations, rather than focusing primarily on the destruction of physical capital. In these respects, the concept of social capital shows considerable promise.

Moving back to disaster-related topics, there are a number of possibilities where social capital theory might be helpful. First, emergence here has been treated, mostly implicitly, as indicating the creation of new social capital. It would be useful to examine the literature on emergence, scattered through the disaster literature, to examine the outcome. Second, social capital theory might be useful in an analysis of the problems of external aid in disaster since such aid disrupts existing obligations, distorts informational potential, and imposes new authority patterns. Third, social capital theory is useful in the way it links microanalysis with macro-analysis. Most psychological studies of disaster victims have focused on psychodynamic causation with borrowed concepts, such as Post-Traumatic Stress Syndrome. Such theoretical approaches have been largely unsuccessful. Since social capital theory links the consequences of individual action to social resources, such a linkage holds the possibility of explaining individual "trauma" and individual resilience to disaster.

Conceptually, social capital theory can be useful in comparative studies, both at the community level and at a social level. It might be useful to examine communities that have persisted and grown in situations that are now seen as high risk, and have led to enduring disaster subcultures. More complex, of course, are historical and comparative studies. As Gregory Bankoff has suggested:

> Perhaps the whole notion of threat is so interwoven into the pattern of historical development and daily life that many aspects of culture perceived as distinctive have their origins, at least, partly in the need for collective action in the face of common dangers.[43]

Russell R. Dynes *is Research Professor in the Disaster Research Center (DRC) of the Department of Sociology at the University of Delaware. He is the co-founder and former Co-Director of DRC. From 1976-79, he chaired the Committee on International Disaster Assistance, National Academy of Sciences/National Research Council and in 1979, he served as head of the Task Force on Emergency Preparedness and Response*

for the President's Commission on the Accident at Three Mile Island. From 1986-90, he served as President, Research Committee on Disasters, International Sociological Association. Dr. Dynes is author or editor of eleven books, including Organized Behavior in Disaster*;* Sociology of Disaster; Disasters, Collective Behavior and Social Organization *and* The Handbook of Disaster Research.

[1] See Russell R. Dynes, "Finding Order in Disorder: Continuities in the 9-11 Response," *International Journal of Mass Emergencies and Disasters* 21, no. 3 (2003): 9-23, and Edgar Jones, Robin Woolven, Bill Durodie and Simon Wessley, "Public Panic and Morale: Second World War Civilian Responses Re-examined in the Light of the Current Anti-terrorist Campaign," *Journal of Risk Research* 9, no. 1 (2006): 57-73.

[2] City of Oklahoma City, *Alfred P. Murrah Federal Building Bombing April 19, 1995, Final Report* (Stillwater, OK: Fire Protection Publications, Oklahoma State University, 1996).

[3] National Institute of Standards and Technology, "NIST and the World Trade Center" (May 26, 2006). Available at http://wtc.nist.gov/ .

[4] See, for example, Havidan Rodriquez, E.L. Quarantelli and Russell R. Dynes, eds., *Handbook of Disaster Research* (New York: Springer, 2006).

[5] James Coleman, *Foundations of Social Theory* (Cambridge, MA: Belknap Press, 1990).

[6] See E.L. Quarentelli, "Panic Behavior: Some Empirical Observations," in *Human Response to Tall Buildings* (Stroudsburg, PA: Dowden, Hutchinson and Ross, Inc., 1997), 336-350.

[7] Russell R. Dynes, *Organized Behavior in Disaster* (New York: Lexington Books, 1970). Republished in 1972 by the Disaster Research Center.

[8] Thomas Drabek, "Emergent Structures," in Russell Dynes, B. De Marchi and C. Pelanda, eds., *Sociology of Disaster: Contributions of Sociology to Disaster Research* (Milan: Franco Angeli, 1987), 262.

[9] James Coleman, "Community Disorganization," in Robert Merton and Robert Nisbet, eds., *Contemporary Social Problems* (New York: Harcourt Brace and World, 1961), 573-574.

[10] This process is described in more detail in Dynes, *Organized Behavior.*

[11] Russell R. Dynes, "The Concept of Role in Disaster Research," in Dynes, et al, eds., *Sociology of Disaster,* 71-102.

[12] The generic term "family" covers a variety of structural arrangements. As the term is used here, however, the emphasis is on the affective element in the relationship, which cuts across different structural arrangements.

[13] B.E. Aguirre, Dennis Wenger, Thomas A. Glass, Marceline Diaz-Murillo, and Gabriela Vigo, "The Social Organization of Search and Rescue: Evidence from the Guadalajara Gasoline Explosion," *International Journal of Mass Emergencies and Disasters* 13 (1995): 93-106.

[14] Michael Lechat, "Corporal Damage as Related to Building Structure and Design," *Center for Research on the Epidemiology of Disaster,* Catholic University (Belgium: Lovain, 1989).

[15] Ibid.

[16] Aguirre, et al., "Social Organization of Search and Rescue."

[17] Joseph Scanlon and Richard Hiscott, *Making the EMS System Fit the Plan: Individual Behavior and Organizational Response* (Ottawa: Emergency Communication Research Unit, Carleton University, 1990).

[18] Thomas Drabek, *Human System Response to Disaster* (New York: Springer-Verlag, 1986), 114.

[19] Anne Whyte, *Survey of Households Evacuated During the Mississauga Chlorine Gas Emergency, November 10-16, 1979* (Toronto: Emergency Planning Project, Institute for Environmental Studies, University of Toronto, 1980).

[20] Ronald W. Perry, "A Model of Evacuation Compliance Behavior," in Russell R. Dynes and Kathleen Tierney, eds., *Disasters, Collective Behavior, and Social Organization* (Newark, DE: University of Delaware Press), 85-98.

[21] The negative implications of obligations can be illustrated in societies in which they are structured along caste and religious lines. In a report concerning an earthquake in India (CNN.com, Feb. 8, 2001) it was indicated when relief groups arrived at Lakhond, Gujirat, they were shown six different tent cities occupied by different Hindu castes, untouchables, outside the caste system, and Muslims. The structuring

forced a competitive struggle among the various communities for resources, even though officially such caste divisions have been considered illegal for years. So social networks can enhance or impede the restoration of social order.

[22] Russell R. Dynes, E.L. Quarantelli, and Dennis Wenger, *The Organizational and Public Response to the September 1985 Earthquake in Mexico City, Mexico* (Newark: DE: Disaster Research Center, 1988).

[23] Colleen Fitzpatrick and Dennis Mileti, "Public Risk Communication," in Dynes and Tierney, eds., *Disasters, Collective Behavior, and Social Organizations,* 71-84.

[24]Ibid, 82.

[25] Perry, "A Model of Evacuation."

[26] Allan Barton*, Communities in Disaster: A Sociological Analysis of Collective Stress* (New York, Doubleday & Company, 1969).

[27] See E.L. Quarantelli, "The Nature and Conditions of Panic," *American Journal of Sociology* 60 (1954): 267-275, and Quarantelli, "Panic Behavior."

[28] This does not mean that looting may not be problematic in certain situations, frequently called disasters. For example, certain situations, such as urban riots and or ethnic conflict, are by their very nature conflict situations and the appropriation and destruction of property reflects that conflict. "Natural" disasters are consensus situations since there is agreement that property losses are "bad" and externally caused. (For further elaboration on this, see E. L. Quarantelli and Russell R. Dynes, "Dissensus and Consensus in Community Emergencies: Patterns of Looting and Property Norms," *Il Politico* 34 (1969): 276-291).

[29] E.L. Quarantelli and Russell Dynes, "Looting in Civil Disturbances: An Index of Social Change," *American Behavioral Scientist* 11 (1968): 7-10.

[30] Dennis Wenger, "DRC Studies of Community Functioning," in *Proceedings of the Japan-United States Disaster Research Seminar: Organizational and Community Responses to Disasters* (Newark, DE: Disaster Research Center, 1972), 39.

[31] Social capital as exemplified in organizations has not been explored extensively, but a major potential exists in the work of Gary Kreps. See *Social Structure in Disaster* (Newark, DE: University of Delaware Press, 1989) and Gary A. Kreps and Susan Bosworth, *Organizing, Role Enactment and Disaster* (Newark, DE: University of Delaware Press, 1994). Also Gary Webb, "Role Enactment in Disaster: Reconciling Structuralist and Interactionist Conceptions of Role," Ph. D. Dissertation, University of Delaware, 1998.

[32] See Thomas R. Forrest, "Group Emergence in Disasters," in E.L. Quarantelli, ed. *Disasters, Theory, and Research* (Beverly Hills, CA: Sage, 1978); Drabek, *Human System Response to Disaster*; Kreps, *Social Structure and Disaster*.

[33] Louis A. Zurcher, "Social Psychological Functions of Ephemeral Roles: A Disaster Work Crew" *Human Organizations* 27 (1969): 281-297.

[34] See Dynes, *Organized Behavior in Disaster.*

[35] Russell R. Dynes, "The Lisbon Earthquake of 1755: the First Modern Disaster," in Theodore E.D. Braun and John B. Radner, eds. *The Lisbon Earthquake of 1755: Representation and Reactions* (Oxford: Voltaire Foundation, 2005), 34-50.

[36] E.L. Quarantelli, "Disaster Management, Emergency Management and Civil Protection: The Historical Development of Organized Efforts to Plan for and Respond to Disaster," Preliminary Paper No. 301 (Newark, DE: Disaster Research Center, 2000), 13.

[37] Russell R. Dynes and E.L. Quarantelli, *The Role of Local Civil Defense in Disaster Planning* (Newark, DE: Disaster Research Center, 1977),17.

[38] Ibid., 39.

[39] For a more detailed discussion, see Thomas Drabek, "Evolution of Emergency Management," 3-29, and Gary Kreps, "Organizing for Emergency Management," 30-54, in Thomas Drabek and Gerald J. Hoetmer, eds., *Emergency Management: Principles and Practices for Local Government* (Washington: International City Managers Association, 1991). Also Richard T. Sylves, "Redesigning and Administrating Federal Emergency Management," in Richard T. Sylves and William Waugh, eds. *Disaster Management in the United States and Canada* (Springfield, IL: Charles C. Thomas Publisher, Ltd. 1996), 5-25.

[40] Department of Homeland Security, *National Response Plan* (Washington, DC: Government Printing Office, December 2004).

[41] E.L. Quarantelli, "Catastrophes are Different from Disasters: Some Implications for Crisis Planning and Managing Drawn from Katrina" (2005) and Russell R. Dynes and Havidan Rodriguez , "Finding and Framing Katrina: The Social Construction of Disaster" (2005). At http://understandingakatrina.ssrc.org/

[42] Kathleen Tierney, "Not Again: Recycling Disaster Myths in the Aftermath of 9/11," Special Session: Annual Meeting of the American Sociological Association, Chicago, Il. August 17, 2002, 11.

[43] Gregory Bankoff, "Rendering the World Unsafe: Vulnerability as Western Discourse," *Disasters* 35 (2001): 30.

Risk Perception and Terrorism: Applying the Psychometric Paradigm

Clinton M. Jenkin

THE PSYCHOLOGICAL NATURE OF RISK

Suppose for a moment that the New York Port Authority receives a threat of a radioactive "dirty bomb" to be detonated on a container ship in the Port of New York. Lower Manhattan is evacuated, and most of the other five boroughs' residents also choose to leave. Business grinds to a halt as both consumers and workers take cover. Within thirty-six hours, the Department of Homeland Security (DHS) announces that the threat has passed. However, many residents wait several more days before returning, while others do not return at all. Business continues to wane as tourism stalls and factories and shops close down. It will be several months before the city fully recovers. This illustration demonstrates the importance of perceived risk regarding terrorism. The perception of risk – whether or not risk is actually present – is sufficient to cause real and long-term damages. Understanding how specific factors drive the perception of risk is essential to understanding how people will respond to threats of terrorism.

There are many benefits to the empirical study of risk perception among the general populace. This research provides a better understanding of how risk perception influences political attitudes; it provides insight into how risk perception impacts various behaviors; it allows the mapping of social processes such as risk amplification and attenuation; it informs the development of effective communication and education programs; and it is useful for identifying which situational factors contribute to perceived risk. Each of these benefits will be discussed in turn, along with an examination of previous contributions in this field and explanations of how they inform homeland security research and policy.

The concept of risk is a psychological one. Risk, as opposed to danger, is a socially constructed phenomenon.[1] Riskiness is based on perception rather than fact, and this perception is based on qualitative, not quantitative characteristics of the hazard being considered.[2] Paul Slovic argues that risks are made up of qualitative attributes like voluntariness or probability. He further posits that no single attribute defines the risk of a particular hazard; neither are specific attributes equally influential across different hazards.[3] Even when the facts and probabilities of a particular hazard are well defined and well known, human judgment is required to determine which information is most important to defining the risk of that hazard. A study by Slovic and others found that participants' ratings of risk did not match their own mortality estimates, indicating that factors other than death toll must be related to risk decisions.[4] Whether a risk is considered acceptable is also a matter of priorities and values, which are psychological by definition.[5] The subjective and perceptual nature of risk makes it an important area of study for the psychological sciences.

Perhaps the best illustration of the subjective nature of risk is the discrepancy between expert and lay evaluations of a hazard. When judging the risk of a hazard, experts rely much more heavily on mortality estimates and probabilities than do

laypersons. Slovic and his associates reported that expert judgments of risk corresponded to objective statistical data, whereas layperson judgments did not.[6] Slovic explained such a discrepancy by concluding that experts view risk as the likelihood of actual harm based on mortality estimates, whereas lay perceptions of risk are based on a number of qualitative (and subjective) characteristics.[7] Some of the characteristics linked to lay perceptions of risk include the voluntariness of exposure, the dread associated with the hazard, the extent to which the risk can be controlled, the potential for catastrophe, the level of uncertainty associated with the hazard, and the perceived inequality of risk/benefit distribution.[8] It is well-documented that expert and lay judgments of risk are different; this difference can be traced to qualitative dimensions of risk that are applied to lay judgments, but not to expert judgments. The inconsistency between expert and lay judgments of risk demonstrates the psychological nature of risk.

This inconsistency also creates a debate about the appropriateness of using expert evaluations alone for policy decisions. In most cases, government and business policy makers rely almost exclusively on quantitative risk assessment to guide policies. In many cases the involved public fails to accept such assessment. One example is nuclear power generation, which has been largely rejected in this country even though it is both safer and cleaner than fossil fuel alternatives. Another example is the decrease of property values near toxic waste sites, despite repeated assurances that the materials have not and will not impact local residents. Participants in a study conducted by Donald MacGregor and Paul Slovic considered the standard cost-benefit analysis used by experts to be morally insufficient for evaluating and regulating risk, but acceptable as part of a more subjective evaluation process.[9] Abraham Wandersman and William Hallman agreed that such analysis was insufficient for a number of reasons. First, quantitative risk assessments are based on a number of assumptions that introduce uncertainty into the process; second, the credibility of the risk assessors may be suspect; and third, expert assessment often fails to consider issues that are important to the public interest.[10] The unwillingness of the public to accept expert risk assessment is a further demonstration of the psychological nature of risk.

In summary, the concept of risk is socially constructed and psychologically oriented. Comparisons of expert and lay judgments of risk illustrate that public assessments of risk are tied to qualitative, rather than quantitative, characteristics of a hazard. The relative importance of these qualitative characteristics varies across people or across hazards. Risk perception research techniques can identify which characteristics are important and when. The question of using only expert judgments for policy decisions involving risk is especially salient in the area of terrorism. The Department of Homeland Security is engaged in various projects designed to objectively assess risk. Whether such assessments will be adequate to provide public support for policy decisions is far from certain.

By itself, keeping people safe is not sufficient: they must also feel safe. The importance of this point in implementing homeland security and emergency preparedness programs is difficult to overstate. Without a perception of safety, voters will locate and authorize new leaders (both local and federal) who share their priorities, and will implement a more "acceptable" security policy. Such a potential action is not just a political threat; it can have a serious negative impact on legitimate programs that are effectively reducing risk, and divert money to programs that increase the feeling of safety without increasing actual safety. The answer, from the standpoint of authorities

attempting to minimize risk and maximize recovery, is to find a middle ground between measures that reduce objective risk and measures that reduce perceived risk. Risk perception research can inform policy makers on how to balance objective assessments with public opinion regarding security priorities.

BENEFITS OF RISK PERCEPTION RESEARCH

Slovic uses the Ford Pinto as a case study to illustrate the value of understanding risk perception. After producing and selling the Pinto, Ford discovered that a defect in the fuel tank could cause the car to catch fire. Ford did a cost-benefit analysis and concluded that a recall would be too expensive. If Ford had considered perceived risk in the analysis they might have made a different decision.[11] Declining to fix the problem via a recall resulted in a public relations nightmare that cost Ford much more than a recall would have. Even though the actual fires did not create a significant economic problem, the perception that Ford's product might catch fire did. The mere perception of a threat was enough to cause severe problems. The same holds true for terrorism. If a terrorist organization provided a credible threat that a nuclear bomb would detonate in New York Harbor, the resulting evacuation and general atmosphere of the city would cripple the state and perhaps the national economy, independent of whether the danger was real. Understanding risk perceptions and responses to risk is vital to understanding – and ultimately affecting – public responses to terrorism.

Risk Perception and Political Attitudes

The study of risk is important in several ways. The first benefit to studying risk is that it allows psychologists to better understand political attitudes. Perceptions of risk drive public priorities.[12] As in the case of the Pinto, or nuclear energy, or airline security, the perception of risk – rather than actual danger – drives public demands for action. This phenomenon is demonstrated in cases of environmental hazards. Public perceptions of risk seriously affect management and regulatory organizations' budgets, agendas, and priorities.[13] For policymakers, especially elected policymakers, the psychological impact of environmental hazards is just as important as the physical impacts.[14] Thus, perceptions of risk are an important component of political attitudes.

Brian Gerber and Grant Neeley studied how perceived risk of routine hazards was related to attitudes about government regulation. They found that increased perceived risk of a hazard was positively related to support for regulation of that hazard, even when the cost of such regulation was stated to be significant. Two other variables affected this relationship: issue awareness and trust in the regulators. If respondents considered themselves to be ill-informed on an issue, there was no relationship between perceived risk and support for regulation. Trust moderated the relationship between perceived risk and support for regulation; if the respondents did not trust the regulators, then they were less likely to support regulation, even if perceived risk was high.[15] These results also apply to terrorism. Leonie Huddy and associates found that levels of perceived risk were linked to willingness to support aggressive anti-terrorist policies.[16] Studying which features of a terrorist hazard affect perceptions of risk allows policymakers to understand which terrorist hazards are likely to become important to the public and why. In our democratic society understanding public priorities is essential to developing a politically acceptable action plan.

Risk Perception and Behaviors

The second benefit of studying risk is that researchers can understand how perception of risk impacts behaviors.[17] Along with Ellen Cohn, the author has documented that perceived risk of terrorism was positively related to adaptive behaviors such as having an emergency supply kit.[18] Similar studies have found this relationship to hold true for fear and perceived risk of crime as well.[19] J. Sherwood Williams and others, in a study of urban adolescents, found that fear of crime was an important predictor of defensive behaviors such as going out in groups, learning self-defense, carrying spray, or carrying a safety whistle.[20] Paul Lavrakas compared suburban and urban dwellers and found that urban dwellers, who had a higher fear of crime, restricted their behavior more than the subjects living in the suburbs.[21] David McDowell found a positive link between fear of crime and gun ownership.[22] Gustavo Mesch found that an increase in perceived risk was indicative of a decrease in nighttime activities.[23] The behavioral effects of perceived risk and fear of crime are well documented, though the research has not differentiated behavioral changes related to fear from those related to perceived risk. Numerous behavioral changes were also observed after 9/11, though it is unclear which of these changes were caused by perceived risk.[24] Identifying the extent to which perceived risk changes behaviors is an important goal of risk researchers.

Risk Amplification and Attenuation

The third benefit to studying risk is that it can clarify the conditions under which perceptions of risk either increase or decrease. Risk researchers have developed a descriptive mechanism known as risk amplification. Risk amplification is concerned with factors, both personal and social, that create either a heightened or lowered sense of risk within a society.[25] Risk amplification ties reactions to socio-economic processes as well as event characteristics.[26] This framework considers issues such as the stigma associated with a hazard, assignment of blame, and the social dynamics within a society in order to understand why a risk might become over- or under-estimated.[27] Understanding the complex interplay between perceptions of risk and social processes is an important contribution of risk research, and can inform communication and policy decisions regarding risk.

The social amplification of risk framework can be a useful tool for tracing the social evolution of attitudes toward terrorism. Consider that several major terrorist attacks occurred that involved U.S. citizens before 9/11, such as the two previous World Trade Center bombings, the Oklahoma City Bombing, the Marine barracks bombing in Lebanon, and the dual U.S. Embassy bombings in Kenya and Tanzania. Counter-terrorism did not become a national priority, however, until after 9/11. While the damage of the 9/11 attacks is one variable, the risk amplification framework provides a mechanism for understanding what other social factors were involved in alternately keeping terrorism in the background for a time and then thrusting it onto an international center-stage.

Risk Perception and Communication

The fourth benefit of studying risk is that an understanding of risk perceptions is vital to developing proper communication and education strategies.[28] It is important for decision makers and enforcement officials to be able to explain any hazard and the related course of action to the public. Educational initiatives must also build an accurate and useful public awareness base. Neither of these goals can be accomplished unless communicators understand how risk is defined and perceived by the public. In the case of terrorism, communication is particularly important because any major warning must be accompanied by instructions, and those instructions must be heeded by the public at large.

Several factors are known to impact risk perception. The first and most important is trust, which has been repeatedly linked to perceived risk. Margaret Heldring identified credibility as the first requirement for effective risk communication.[29] Trust in information source was found to impact perceived risk of environmental health hazards.[30] In a study that manipulated various features of communication of risk, the manipulations were not as important as issues of trust in government and authority.[31] Trust seems to be more important when communicating hazards about which the perceiver has little knowledge.[32] Any communication or education initiative that lacks credibility will have minimal effect on perceptions of risk. It is vital that agencies and persons responsible for communicating terrorism information to the public maintain this trust, or any directions concerning evacuation, sheltering, et cetera, stand a fair chance of being ignored by the public.

Lennart Sjöberg suggested that the issue of trust may explain why lay person risk perceptions seem irrational to experts; if the experts themselves lack credibility, then disbelieving their assurances is the only rational response.[33] Slovic addresses systemic influences that destroy trust. These influences are noticeably present in the arena of terrorism. One, failures are more noticeable than successes. This is especially true for the war on terror, where most successes cannot be identified or publicized because such information might compromise intelligence sources. Two, failures are given greater weight than successes, even if salience is equal. With regards to terrorism, the costs of failure are much more noticeable than are the benefits of success, because success merely preserves the status quo. Three, once an audience loses trust, it screens future perceptions. Failures become even more noticeable, because people tend to retain information consistent with their attitudes.[34] Julie Barnett and Glynis Breakwell use the 1995 contraceptive pill scare in England to illustrate how contradictory expert testimony erodes credibility and inflates risk.[35] Due in part to the 24-hour news cycle, the American public is treated to constant contradictory "expert" testimony. While trust is an extremely important variable in risk communication, it is also a very fragile one.

Specificity is another communication factor that impacts perceptions of risk. Risk communications that are not specific are more likely to increase anxiety without increasing awareness.[36] One example of the importance of specificity in terrorism communication is the color-coded alert system used by the Department of Homeland Security (DHS). For law enforcement officials, this alert system is marginally useful, if each level of alert is accompanied by specific actions and procedures. Such procedures are developed at the local level, however, so the DHS system by itself is only useful if the local jurisdictions have attached their own set of specifics. More useful to local authorities is information received through law enforcement channels such as Law

Enforcement Online or the FBI's Joint Terrorist Task Force gateway; this information is more useful precisely because it is more specific. For the general public, the DHS color-coded system is rightfully criticized for being counterproductive, precisely because it offers no useful information to a public audience.

Heldring outlined criteria for risk communication to be considered useful: credibility, specific information about the risk, specific information about what is being done by authorities, specific information about what the audience should do, and empathy.[37] In the case of terrorist warnings, unfortunately, such specific information is usually unavailable, or cannot be shared with the public. But risk research provides insight into how terrorist warnings should ideally be constructed and relayed.

Barnett and Breakwell postulated a mechanism by which past risk communications influence the response to further risk communications. The series of previous hazard notifications (a hazard sequence) impacts the way a hazard is normalized; this normalization results in a hazard template – a social heuristic that speeds the processing of information related to the hazard. The hazard template is the public's conception of the hazard and includes such characteristics as the organizations responsible, potential victims, causes, and consequences; this template provides a common ground for interpersonal communication about the hazard. Barnett and Breakwell conclude that in order to understand how people will react to a future risk communication, we must first understand how previous communications have shaped the audience's hazard template.[38] Because so much of the average person's experience with terrorism is from media messages, it would be useful to examine how these messages have constructed the hazard template of "terrorism" and how this template filters new messages.

Situational Factors

A fifth benefit to studying risk is to identify situational factors that influence risk perception. Psychological research has identified four situational factors that influence how people judge risk: expected loss, catastrophic potential, other qualitative characteristics (these will be discussed in greater detail below), and beliefs about cause.[39] Risk perception research provides insight into which event or situational features will be most important for particular hazards. In the case of terrorism, such information assists researchers or public officials – given specific information about the characteristics of a terrorist threat – to predict how people might react to that threat.

Personal Factors

Several intra-personal factors have been linked to risk perception. In the health psychology literature, three factors have been associated with risk perception: demographics, socio-psychological variables (like those discussed previously regarding responses to terrorism), and structural variables such as experience with the hazard or depth of knowledge.[40] Sjoberg postulates that certain individuals may demonstrate a greater sensitivity to risk, and this possibility deserves empirical analysis.[41]

Slovic linked risk judgments to gender (women judge risk to be higher), race, (minorities judge risk as higher), political worldview, personal affiliations, emotional affect, and trust (as outlined above). Upon closer inspection, however, it appears that race and gender differences in perceived risk can be tied to the "white male effect."

About one-third of white men have much lower risk judgments than everyone else, regardless of gender or race; when these responders are excluded from analyses, race and gender differences become non-significant. Examining these low-risk respondents reveals that they tend to be well-educated, have high socioeconomic status, conservative political orientation, and higher trust in authority.[42] The white male effect may provide a link to other personal factors that influence risk perceptions. Fortunately, intra-personal variables is one area in which terrorism attitude researchers have acquired a great deal of useful information; as previously discussed, however, most of the research failed to differentiate between reactions to past events and reactions to potential events. The risk literature provides the empirical background to devise and test specific hypotheses regarding potential terrorism and personal variables.

In sum, studying risk perception is beneficial in many ways. It provides insight into how risk perception is related to attitudes and lifestyles. It provides a framework for understanding how risk is amplified or attenuated across a culture. It allows for the proper development of effective communication and education strategies and it provides an understanding of situational and personal factors associated with risk perception. The natural inclination of the individual is to reduce risk. It is an important contribution of psychology to provide empirical analysis of how and why risk is perceived, and what consequences are associated with risk perception.

THE PSYCHOMETRIC PARADIGM

The psychometric paradigm was developed as the research paradigm that logically follows the assumption that risk is psychologically determined. The primary assumption of the psychometric paradigm is that risk is inherently subjective.[43] Recall the importance of qualitative hazard characteristics to lay perceptions of risk. The psychometric paradigm is based on techniques that collect and analyze subjective rating of these qualitative characteristics, including both global (e.g. riskiness, etc.) and dimensional (e.g. controllability, familiarity, etc.) evaluations of particular hazards.[44] These subjective ratings then form a sort of personality profile for each hazard being studied. It is this pattern of qualitative ratings that affect perceptions of risk. Psychometric studies have discovered five factors that generally account for risk perceptions: qualitative features of the hazard, benefits of the hazard, annual mortality rates, catastrophic mortality potential, and relative mortality seriousness.[45] For the purposes of the proposed studies, the factor of greatest interest is the qualitative features, or personality profile, of the hazard itself. An understanding of how these qualitative ratings impact perceptions of risk is a vital step in understanding attitudes toward terrorism.

Dimensions and Factors of Risk

Psychometric studies have studied numerous dimensions of risk for scores of hazards. Dimensions commonly used are listed in Table 1. Obviously, so many dimensions can lead to very cumbersome research designs, so most risk studies include the dimensions most applicable to the study at hand. For example, a terrorism study may elect to exclude inequitability, because the inequity of terrorism risk is not likely to be an issue as it might be for the risks of a toxic waste dump or nuclear power plant.

Table 1

Qualitative Dimensions of Risk Used in the Psychometric Paradigm[46]

Voluntariness	The extent to which exposure to the hazard is voluntary.
Immediacy	The extent to which the consequences are noticed immediately.
Knowledge of exposure	The extent to which a person knows if he has been exposed.
Expert knowledge	The extent to which experts know about the hazard.
*Controllability**	The extent to which a victim can control the severity of consequences due to exposure.
Novelty	The extent to which the hazard is new to society.
*Catastrophic potential**	How many fatalities occur at once.
*Dread**	The extent to which the effects of exposure are dreaded.
*Severity**	The extent to which the consequences of exposure are severe.
Delayed	The extent to which the consequences of exposure are delayed.
C*ertainly fatal**	The extent to which exposure will definitely cause fatality.
*Increasing**	The extent to which the risk is increasing over time.
*Preventability**	The extent to which the hazard is preventable.
*Inequitable**	The extent to which risks and benefits are not equally distributed across society.
*Affects future generations**	The extent to which the hazard will affect future generations.
*Global catastrophe**	The extent to which the hazard threatens a global catastrophe.
*Easily reduced**	The extent to which risk associated with the hazard can be easily reduced.
*Personal impact**	The extent to which the risk affects the respondent personally.
Observability	The extent to which the effects of exposure are observable.

Dimensions marked with an asterisk (*) were directly correlated with perceptions of risk.[47]

Risk studies have also sought to reduce the number of analyses by reducing these qualitative dimensions into factors via factor analysis. This approach has been very successful and has lead to robust research findings. Two factors have been consistently (though not exclusively) identified: *dread risk*, which is associated with lack of control, dreaded consequences, catastrophic potential, inequitable distribution, increasing risk, and fatal consequences; and *unknown risk*, which is associated with unobservability, novelty, unknown exposure, unknown to science, and delayed consequences.[48] Two other factors have also been identified in individual studies: number of people exposed

and severity of consequences.[49] The most consistent finding, however, is that the dread risk factor has been the best predictor of the overall perceived risk of a hazard.[50] Identifying the importance of dread and its impact on perceptions of risk is a valuable contribution of risk research in general and the psychometric paradigm in particular.

The identification of two primary factors that qualitatively described hazards has allowed risk researchers to map out a number of hazards in two-factor space. Such taxonomy is useful for two purposes. The first value is that it explains differences in risk perceptions across hazards. In fact, the perceived risk of a hazard is related to its position in the two-factor space. The second value is that it explains discrepancies between lay and expert estimates of risk. While lay perceptions of risk are consistently tied to dread risk, expert ratings are not.[51]

One risk judgment that merits special attention is signal value. An event is high in signal value if its occurrence changes the perceived probability of future occurrences.[52] For example, 9/11 was extremely high in signal value because it was taken as evidence that such attacks were more likely than before to occur again. In contrast, a suicide bomber on a bus in Tel Aviv has a low signal value, because this occurrence does not alter perceptions of how likely it is to occur again. Along with overall perceived risk, signal value has been linked to the position of hazards within a two-factor space.[53] Differences in signal value appear to account for differences in ratings of worry, need for awareness, and need for preventative efforts.[54] Signal value is also related to how well known a hazard is; new hazards tend to be higher in signal value. Signal value may be an important political consideration as well, because a hazard with high signal value is particularly open to risk amplification processes.[55] Barnett and Breakwell suggest that novel information is key to intensifying perceived risk, while confirmatory information has little impact on risk perception.[56] Signal value is an important variable in risk perception. Given the extremely high signal value of 9/11, this concept should be an important consideration in any study of attitudes toward terrorism.

In sum, the psychometric paradigm is a research methodology derived from the assumption that risk is subjective and that qualitative features of hazards will be linked to perceptions of risk. Numerous qualitative features (dimensions) have been studied; some are consistently related to risk and some are not. One of the most relevant features to terrorism hazards is signal value. These dimensions can also be reduced to underlying factors – dread and unknown risk. These two factors allow the hazards to be mapped on a Cartesian plane. The location of each hazard is useful for understanding how it is perceived. This paradigm provides a promising set of techniques with which to better understand attitudes toward terrorism. Researchers may be able to develop "personality profiles" for different attacks, profiles which in turn could lead to the creation of a taxonomy of terrorism based on subjective evaluations.

The Psychometric Paradigm and Specific Hazards

While most psychometric studies have examined many different hazards, the paradigm can be adapted to accommodate an in-depth study of one hazard. Single hazard domains have been studied using the psychometric paradigm, and they too can be represented in two-factor space, where position is predictive of perceived risk.[57] Slovic examined attitudes toward unwanted land uses and also provided several examples of hazards that have been studied using psychometric techniques to specific hazards, such as automobile structural defect, railroad accidents, and automobile subsystem failures.[58]

While in these studies risk dimensions were reducible into factors, the factors did not always match those found in multiple-hazard studies; for example, the factors observed for automobile subsystem defects were "foreseeable" and "severe, uncontrollable damage."[59] Given the nature of the hazard, these factors are more logical than dread risk and unknown risk, the factors discussed above. The psychometric paradigm has also been successfully applied to single hazards, but Slovic cautions against representing complex events as a single homogenous data point.[60] While terrorism has been included as a single hazard in past psychometric studies, the complexity and relevance of terrorism in today's society merits an empirical exploration of terrorism as the entire hazard space.

APPLICATION TO HOMELAND SECURITY/EMERGENCY PREPAREDNESS

Based on the principles outlined above, several recommendations can be made for those directly involved in homeland security, emergency preparedness, and disaster recovery. These recommendations are purposely general, because the specifics of how to implement them will vary from one context to another. This list is not intended to be exhaustive; surely other recommendations can be made, again based on a specific context. The following do provide, however, a framework within which to apply the research cited here.

First, it is essential for an organization to build trust with its audience/constituents. Without trust, any information from that organization will likely be discounted, including information about levels of safety, disaster scenarios, or evacuation procedures. One important aspect of gaining and/or maintaining trust is to make the successes of an organization as visible as possible. This task is more difficult than it sounds, because the failures of any organization are generally more apparent and noticeable than are its successes. In some cases, particularly with intelligence organizations, successes cannot be shared with the public because such information may compromise future efforts. But it is essential that agencies involved with homeland security have proactive campaigns designed to build trust with the public by actively communicating information favorable to the agency. Agencies can also build trust in the way that they deal with failures. Open communication about the cause of a failure, and steps being taken to prevent another, can and should be used to rebuild trust after an agency fails to meet its responsibilities.

A psychological phenomenon that naturally inhibits trust is hindsight bias, or the "I-knew-it-all-along" phenomenon. Once an event has occurred, observers tend to overestimate the predictability of the event. This phenomenon means that failures are not only more noticeable, they are considered to be inexcusable, especially failures of foresight. From the public's perspective, any catastrophe or disaster could have been avoided, because there was sufficient evidence beforehand that it was going to occur. From an agency's perspective, the evidence predicting an event was buried within the evidence against the event occurring, and thus no foresight was possible. Agencies, and especially their press liaisons, must be aware of this difference in perspective and be ready to publicly account for it.

Second, agencies must offer specific information whenever possible. This point is particularly salient for organizations tasked with motivating people to take action. People tend to ignore general instructions that do not include specific actions. Of course,

the actions requested must also be sensible to the public, or even specifics will be ignored. Therefore agencies must not only provide specific instructions, but give detailed (and simple) explanations for those instructions. Specific information is also needed for warnings. As discussed above, the color-coded system is largely useless to the general population because of its lack of specificity. If details cannot be given, the agency must consider whether releasing general instructions or warnings will actually cause harm to their communication efforts, either through creating distrust among the public, or through desensitizing their audience to such communication. In some cases, it may actually be advisable to present no information rather than to present information that the audience cannot use.

Third, organizations must understand the public's priorities. In cases of general homeland security or emergency preparedness issues, public opinion polls can offer a basic level of insight. In more specific cases, some level of primary research may need to be conducted in order to identify priorities. Once an organization can understand the perspective (and thus the priorities) of its constituents, they are better prepared to address those priorities. Often an agency is already addressing these priorities, and it simply needs to do a better job of communicating these efforts to the public. In other cases the public priorities may need to be altered; this is a very difficult thing to do, but it is possible if the issues of trust and specificity have already been addressed. If an agency does find it necessary to conduct a campaign to alter the public priorities, awareness of public opinion will inform decision makers of the progress of such a campaign.

Fourth, the qualitative dimensions (and responses to them) discussed above should be incorporated into scenario development exercises. Scenario development may be more accurate if the subjective features of a threat are included along with the objective features. Of course, the impact of these subjective features is still a matter of ongoing research, especially in the area of terrorism, so such a process would necessarily be iterative. Once this information is added to our current knowledge and accounted for in predictive models, it should allow for a more sophisticated and accurate prediction of actual behaviors.

CONCLUSION

The study of attitudes toward terrorism is a vital psychological endeavor in the post-9/11 world. Fortunately, much work has been done and the resulting literature provides a great deal of insight into how people respond to terrorism and other threats of violence.[61] Unfortunately, most of the empirical work has focused on responses to past terrorist incidents and has looked mainly at personal factors that are related to such responses.[62] Because each terrorist attack evokes anger and resolve, however, terrorists primarily achieve their goal of fear and intimidation through the threat of future attacks rather than the occurrence of previous ones. From a psychological perspective, the terrorism that has not yet happened is as important as the terrorism that just happened.

Terrorism's future-orientation highlights the importance of understanding how people respond to threats as well as to actual incidents. The best psychological approach to such attitudes is through the field of risk. Risk is based on judgments, and thus is psychological in nature. The psychological study of risk provides insight into how people view various threats, and therefore informs predictions about how people will react to

the threat of terrorism. The psychometric paradigm specifically offers a valuable methodology to explore which features of a terrorist incident drive psychological perceptions and reactions to that incident.

Terrorism – more specifically the threat of terrorism – has become a driving cultural and political force. Credible threat is the currency of terrorist organizations. An organization that cannot threaten and be taken seriously has no power to change attitudes and behaviors. Because the power of terrorism comes from such threats, controlling risk has taken on national significance, with an entire cabinet-level department, as well as local and state-wide partner agencies, devoted to managing (and hopefully reducing) risk. These agencies cannot properly reduce risk, though, without first understanding how risk is perceived. Because of the United States' political structure, public attitudes toward terrorism occupy a pre-eminent place in establishing government priorities. It is essential that psychologists develop empirically-tested knowledge about how these attitudes are constructed, how they change across time, and how they impact behavior. The literature reviewed here provides essential progress toward understanding terrorism attitudes, and outlines a promising framework for continuing that progress.

The author would like to thank the reviewers for their helpful comments, which directly improved this article. This research was supported in part by a graduate student fellowship from the Department of Homeland Security, Office of University Programs, Scholars and Fellows Program. *Correspondence concerning this article should be addressed to Clinton Jenkin, Department of Psychology, University of New Hampshire, Durham, New Hampshire 03824. Email: cjenkin@unh.edu.*

***Clinton M. Jenkin** is a research fellow in the Department of Psychology at the University of New Hampshire. He received his master's degree in Psychology from UNH in 2004, and is now a Ph.D. candidate.*

---

[1] P. Slovic, "Trust, Emotion, Sex, Politics, and Science: Surveying the Risk-Assessment Battlefield," *Risk Analysis* 19 (1999): 689-701.

[2] P. Slovic, "Perception of Risk," *Science* 236 (1987): 280-285.

[3] Ibid.

[4] P. Slovic, B. Fischhoff, and S. Lichtenstein, "Rating the Risks," *Environment* 2, no.3 (1979): 14-20. Slightly revised in P. Slovic, ed., *The Perception of Risk* (Sterling, VA: Earthscan, 2000).

[5] A.H. Wandersman and W.K. Hallman, "Are people acting irrationally? Understanding public concerns about environmental threats," *American Psychologist* 48 (1993): 681-686.

[6] Slovic, et al, "Rating the Risks."

[7] Slovic, "Trust, Emotion, Sex, Politics, and Science."

[8] Slovic, et al., "Rating the Risks."

[9] D.G. MacGregor and P. Slovic, "Perceived acceptability of risk analysis as a decision-making approach," *Risk Analysis* 6 (1986): 245-256.

[10] Wandersman and Hallman, "Are People Acting Irrationally?"

[11] Slovic, "Perception of Risk."

[12] O. Renn, "Concepts of Risk: A Classification," in S. Krimsky and D. Golding, eds., *Social Theories of Risk* (Westport, CT: Praeger, 1992).

[13] Slovic, "Trust, Emotion, Sex, Politics, and Science."

[14] Wandersman and Hallman, "Are People Acting Irrationally?"
[15] B.J. Gerber and G.W. Neeley, "Perceived risk and citizen preferences for government management of routine hazards," *Policy Studies Journal* 33 (2005): 395-419.
[16] L. Huddy, S. Feldman, C. Taber, and G. Lahav, "Threat, anxiety, and support of antiterrorism policies," *American Journal of Political Science* 49 (2005): 593-608.
[17] Renn, "Concepts of Risk."
[18] C.M. Jenkin and E.S. Cohn, "Attitudes toward terrorism: Scale development and implications," *Peace and Conflict: Journal of Peace Psychology* (under review).
[19] K.F. Ferraro, *Fear of Crime: Interpreting Victimization Risk* (Albany: State University of New York Press, 1995).
[20] J.S. Williams, B.K. Singh, and B.B. Singh, "Urban youth, fear of crime, and resulting defensive actions," *Adolescence* 29 (1994): 323-330.
[21] P.J. Lavrakas, "Fear of Crime and Behavioral Restrictions in Urban and Suburban Neighborhoods," *Population and Environment* 5 (1982): 242-262.
[22] D. McDowall, "Firearms and Self-Defense," *Annals of the American Academy of Political and Social Science* 539 (1995): 130-140.
[23] G.S. Mesch, "Perceptions of risk, lifestyle activities, and fear of crime," *Deviant Behavior,* 21 (2000): 47-62.
[24] C. McCauley, "Psychological issues in understanding terrorism and the response to terrorism," in C. E. Stout, ed., *Psychology of Terrorism, condensed edition: Coping with the Continued Threat* (Westport, CT: Praeger, 2004), 33-65; T. Pyszczynski, S. Solomon, and J. Greenberg, *In the Wake of 9/11: The Psychology of Terror* (Washington, D.C.: American Psychological Association, 2003); M. Weidenbaum, "Economic responses to Terrorism," *Executive Speeches* (Oct/Nov 2001).
[25] For a complete treatment of this framework, see N. Pidgeon, R.E. Kasperson, and P. Slovic, eds., *The Social Amplification of Risk* (Cambridge, UK: Cambridge University Press, 2003).
[26] J. Barnett and G.M. Breakwell, "The Social Amplification of Risk and the Hazard Sequence: The October 1995 Oral Contraceptive Pill Scare," *Health, Risk, and Society* 5, no. 3 (2003): 301-314.
[27] J. Flynn, "Nuclear Stigma," 326-352; A. Susarla, "Plague and Arsenic: Assignment of Blame in the Mass Media and the Social Amplification and Attenuation of Risk," 179-206; and T. Horlick-Jones, J. Sime, and N. Pidgeon, "The Social Dynamics of Environmental Risk Perception: Implications for Risk Communication Research and Practice" 262-285, all in Pidgeon, et al., eds., *Social Amplification of Risk*.
[28] Renn, "Concepts of Risk"; P. Slovic, *Perception of Risk from Asteroid Impact*. Paper prepared for the ICSU workshop: "Comet/Asteroid Impact and Human Society," Santa Cruz de Tenerife (November 2004).
[29] M. Heldring, "Talking to the Public about Terrorism: Promoting Health and Resilience," *Families, Systems, & Health* 22 (2004): 67-71.
[30] C. Seguin, L.G. Pelletier, and J. Hunsley, "Predicting Environmental Behaviors: The Influence of Self-Determined Motivation and Information about Perceived Environmental Health Risks, *Journal of Applied Social Psychology* 29 (1999): 1582-1604.
[31] B. Johnson and P. Slovic, "Presenting uncertainty in health risk assessment: Initial studies of its effects on risk perception and trust," *Risk Analysis* 15 (1995): 485-494.
[32] Gerber and Neely, "Perceived Risk."
[33] L. Sjoberg, "Political Decisions and Public Risk Perception," Paper read at the Third International Public Policy and Social Science Conference, St. Catherine's College, Oxford, England (July 1999).
[34] Slovic, "Trust, Emotion, Sex, Politics, and Science."
[35] Barnett and Breakwell, "Social Amplification of Risk."
[36] C.E. Stout, "Using psychology to counter terrorism at the personal and community level," in Stout, ed., *Psychology of Terrorism,* 1-31.
[37] M. Heldring, "Talking to the public about terrorism."
[38] Barnett and Breakwell, "Social Amplification of Risk."
[39] Renn, "Concepts of Risk."
[40] E. Sarafino, *Health Psychology: Biopsychosocial Interactions*, 4th edition (Hoboken, NJ: Wiley, 2002).
[41] Sjoberg, "Political Decisions."
[42] Slovic, "Trust, Emotion, Sex, Politics, and Science."
[43] Slovic, "Perceptions of Risk: Reflections on the Psychometric Paradigm," in S. Krimsky and D. Golding, eds., *Social Theories of Risk* (Westport, CT: Praeger, 1992).
[44] Slovic, ed., *Perception of Risk.*

[45] Slovic, "Perception of Risk from Asteroid Impact."

[46] Sources: B. Fischhoff, P. Slovic, S. Lichtenstein, S. Read, and B. Combs, "How safe is safe enough? A Psychometric Study of Attitudes toward Technological Risks and Benefits," in Slovic, *Perception of Risk*; E.J. Johnson and A. Tversky, "Representations of Perceptions of Risk." *Journal of Experimental Psychology: General* 113 (1984): 55-70; P. Slovic, B. Fischhoff, S. Lichtenstein, "Facts and Fears: Understanding Perceived Risk," in R. C. Schwing and W. A. Albers Jr., eds. *Societal Risk taking: How Safe is Safe enough?* (NY: Plenum, 1980). Excerpts reprinted in Slovic, ed. *Perception of Risk*.

[47] Slovic, et al., "Rating the Risks" and Slovic, et al., "Facts and Fears."

[48] Slovic, *Perception of Risk*; Slovic, "Perception of Risk from Asteroid Impact."

[49]Slovic, Fischhoff, and Lichtenstein, "Facts and fears;" and Fischhoff et al, "How Safe is Safe Enough?"

[50] Slovic, et al., ibid.; Fischhoff, et al., ibid.; Slovic, "Perceptions of Risk: Reflections;" Slovic, "Perception of Risk from Asteroid Impact"; Slovik et al., "Rating the Risks."

[51]Slovic, "Perceptions of Risk: Reflections;" "Trust, Emotion, Sex, Politics, and Science;" "Perception of Risk from Asteroid Impact;" Slovic, et al., "Rating the Risk;" and *Perception of Risk*; Slovic, et al., "Facts and Fears."

[52] Slovic, "Perceptions of Risk: Reflections."

[53] Slovic, *Perception of Risk*.

[54] Slovic, et al., "Facts and Fears."

[55] Slovic, "Perceptions of Risk;" and "Perception of Risk from Asteroid Impact."

[56] Barnett and Breakwell, "Social Amplification of Risk."

[57] Slovic, *Perception of Risk*.

[58] Slovic, "Perceptions of Risk;" P. Slovic, D. MacGregor, and N.M. Kraus, N. N., "Perception of Risk from Automobile Safety Defects," *Accident Analysis and Prevention* 19 (1987):359-373; N.N. Kraus and P. Slovic, "Taxonomic analysis of perceived risk: Modeling Individual and Group Perceptions within Homogenous Hazard Domains," *Risk Analysis* 8 (1988): 435-455.; D.G. MacGregor, D. and P. Slovic, P. "Perceived Acceptability of Risk Analysis as a Decision-making Approach," *Risk Analysis* 6 (1986): 245-256.

[59]Slovic, et al., "Perception of Risk from Automobile Safety Defects."

[60] Slovic, "Perceptions of Risk."

[61] See, for example, W.J.Brown, M. Bocarnea, and M. Basil, "Fear, Grief, and Sympathy Responses to the Attacks," in B. S. Greenberg, ed., *Communication and Terrorism: Public and Media Responses to 9/11* (Cresskill, NJ: Hampton Press, 2002), 245-259; A.M. Miller and M. Heldring, "Mental Health and Primary Care in a Time of Terrorism: Psychological Impact of Terrorist Attacks," *Families, Systems, and Health* 22 (2004): 7-30; L. B. Snyder and C.L. Park, "National Studies of Stress Reactions and Media Exposure to the Attacks," in Greenberg, *Communication and Terrorism,* 177-192; and G. Sprang, "The Psychological Impact of Isolated Acts of Terrorism," in A. Silke, ed., *Terrorism, Victims, and Society: Psychological Perspectives on Terrorism and its Consequences* (Hoboken, NJ: Wiley, 2003), 133-159.

[62] See C.A. Ford, "Living in a Time of Terrorism: What about Older Adolescents and Young Adults?" *Families, Systems, and Health* 22 (2004): 52-53; E.H. Grothberg, "From Terror to Triumph: The Path to Resilience," in Stout *Psychology of Terrorism,* 199-224; and Miller and Heldring, "Mental health and primary care," 161-174.

The National Military Strategic Plan for the War on Terrorism: An Assessment

Nadav Morag

The *National Military Strategic Plan for the War on Terrorism* (hereinafter referred to as the *NMSP* or Plan), released by the Chairman of the Joint Chiefs of Staff (CJCS) on February 1, 2006, sets out the Pentagon's broad strategy for executing, and presumably winning, the Global War on Terrorism (GWOT). The *NMSP* can be viewed as an elaboration of part of the larger and more holistic set of policies spelled out by the Department of Defense (DoD) in its June 2005 *Strategy for Homeland Defense and Civil Support*. The *Strategy for Homeland Defense and Civil Support* envisions a layered approach towards homeland defense and security based on a distinction between: Forward Regions, Approaches to the U.S., the U.S. Homeland and the Global Commons (space and cyberspace).[1] Although the *NMSP* does not specifically position itself within the rubric of the larger June 2005 strategy paper, its focus on attacking terrorist networks abroad, strengthening international governance and creating a global environment inhospitable to terrorists suggest that it should be viewed as a DoD articulation of the "Forward Regions" component of the overall strategy.

This article will focus on the Pentagon's "Forward Regions" strategy through analysis of the *NMSP*. The Department of Defense, of course, recognizes that combating the terrorist threat to the United States and its allies requires an approach that differs in many critical ways from the approaches needed in order to effectively carry out conventional warfare and even counterinsurgency warfare. An effective homeland security strategy, first and foremost, requires the military to "team-up" with civilian intelligence, law-enforcement, and, for specific missions, with emergency service and public health agencies as well. With the exception of the National Guard, much of the military is largely unaccustomed to this effectively unprecedented role in which the Pentagon must "share power" with civilian entities. The Department of Defense has attempted to cope with this quandary by supporting the distinction between "homeland defense" and "homeland security." A cynic might maintain that this distinction has been created in order to enable the Pentagon to retain "ownership" of a major part of the overall effort at securing the American homeland from terrorist threats and, at the same time, to enable it to play an important role under certain circumstances as the lead agency and under others as a supporting agency in domestic security and response activities. Of course, the DoD must also comply with U.S. law (which limits the military's domestic role) and, equally importantly, avoid irritating public and congressional sensibilities with respect to the power and influence, real or perceived, exercised by the military.

Potential motives aside, it is doubtful that many would argue that protecting the United States from terrorism should not require a holistic approach in which the firefighter trained to deal with a possible chemical attack in an American city and the special forces soldier trained to attack terrorist hideouts in some remote

corner of the globe are viewed as part of the same overall mission. The *National Strategy for Homeland Security* recognizes this continuum in its emphasis on prevention, reduction of vulnerability to attacks that do occur, and swift recovery from attacks.[2] Homeland Defense and Homeland Security should not, therefore, be viewed as different strategies, but rather different ends of a continuum that moves from the international arena, to the North American land-mass (and associated offshore areas), to the domestic arena.

Nevertheless, if we attempt to somewhat artificially separate Homeland Defense from Homeland Security, we are still confronted with a lack of clarity as to the precise role the military must play. The DoD's *Strategy for Homeland Defense and Civil Support* places the military in the lead role with respect to "defending the maritime and air approaches to the United States and protecting U.S. airspace, territorial seas, and territory from attacks."[3] However, civilian agencies such as the Federal Aviation Administration and the Department of Homeland Security (via Customs and Border Protection or the U.S. Coast Guard), as well as municipal police departments and county sheriff's departments in border areas, would also be involved in responding to a terrorist attack in American airspace or across a land or maritime border. Furthermore, it is entirely conceivable, particularly with respect to terrorist attacks across land or maritime borders, that non-DoD agencies will not only be the first to respond to such attacks, but may also bring those incidents to their conclusion before the military arrives.

Ostensibly, there is one area of the overall homeland security-homeland defense continuum that lies purely within the military's purview: overseas missions. Here too, however, upon closer inspection, the picture becomes decidedly less clear-cut. Fighting terrorism abroad can be viewed primarily as a warfighting activity and, to the degree that it is such, clearly falls within the purview of a purely military activity (though reports of CIA commandoes operating during Operation Enduring Freedom in late 2001, as well as the global activities of various defense contractors, suggest that even here the military does not enjoy a complete monopoly). Fighting terrorism abroad, can also be viewed as a law-enforcement activity – as it is with respect to coping with terrorist threats emanating from the territory of America's allies (such as those in Europe) or other states operating within the rule of law as legitimate members of the international community. In this context, the military can, at best, play only a minor supporting role. Moreover, as will be discussed below, addressing the terrorist threat in a truly comprehensive manner requires focusing on efforts and delineating policies in areas in which the military has traditionally played little or no role and for which it is unclear that the military possesses or intends to build the capabilities to address these issues.

The upshot of the above argument is that the military, in trying to stake out a role in homeland security, homeland defense and overseas counter-terrorism efforts, has created what is likely to be an impossibly broad and multifaceted "operational area" requiring expertise and experience in so many different *modus operandi* and environments that the Pentagon may be placing itself in danger not only of doing a poor job in areas for which it lacks experience and expertise, but also of losing its core competency skills in the process. In looking strictly at

overseas efforts, the *NMSP* mirrors some of these problems in that it spells out a very broad mission statement, far beyond core military competencies, for coping with overseas terrorist threats.

The *NMSP* is laudable in that it shows an understanding that the terrorist threat is multifaceted and that it encompasses not only military, but political, social, economic, cultural and educational components. However, despite the sophistication of its analysis of the problem, the *NMSP* contains a number of internal contradictions and, more critically, is both unachievable and takes the initiative out of the hands of the U.S. military on the one hand, while on the other, tasks the military with a broad range of largely non-military missions. This article will focus on three central problems and suggest an alternate strategic approach and role for the military likely to be significantly more successful and allow it to fulfill a clearer role within the overall homeland security-homeland defense continuum.

PROBLEM # 1: Goals Unclear and Unrealistic

The Plan sets out the policy goal of defeating violent extremism and creating a global environment inhospitable to terrorists.[4] While this is unquestionably a desirable goal, it is not fundamentally realistic and sets the bar too high with respect to any achievable outcomes for the GWOT. It is highly unlikely that the GWOT will succeed in defeating and/or eradicating violent extremism as a threat to the United States for the foreseeable future and even more unlikely that the global environment can be made inhospitable to violent extremists to the degree that they will be substantially curtailed. The intensity and scope of terrorism may ebb and flow over time due to a range of factors, including effective counter-terrorism policies, but a complete negation of the present Jihadist terrorist threat will, under the most optimistic scenario, take several decades at the least (by which time new terrorist threats may well have emerged).

To illustrate the tenacity of the terrorist phenomenon one need only turn to the Northern Ireland example.[*] The so-called "Real IRA's" attack in Omagh in August 1998 (the single worst terrorist attack carried out in Northern Ireland since the start of the "Troubles," the attack resulted in twenty-nine fatalities and over 300 injuries) serves as one illustration of the tenacity of the terrorist phenomenon in the face of profound and multifaceted efforts made in the political, diplomatic, and military spheres to weaken popular support for terrorist organizations and undermine the infrastructure of those organizations. Despite the ostensible "evolution" of Republican (and Unionist) groups away from terrorism and towards political dialogue, as represented by the 1998 Good Friday Agreement, and despite the findings of the Independent International Commission on Decommissioning under General Sir John de Chastelain in September 2005 that the IRA has put its weapons "beyond use," Britain's Security Service (MI5) was reportedly ordered in May 2006 to devote twenty

[*] Examples of this abound, including the FARC, the PKK, Palestinian Islamic Jihad and other groups who have been the subject of intensive counterterrorism activities and yet continue to pose a threat. Space limitations, however, preclude the provision of additional examples to further substantiate this point.

percent of its already- overstretched resources to disrupting the activities of Republican splinter groups in Northern Ireland.[5]

Consequently, while governments may adopt multifaceted approaches to dealing with the terrorist threat and may be able, over the span of several decades, to significantly impact terrorist organizations and even force some of them to abandon the "armed struggle," there is still no guarantee that even more extreme splinter factions breaking off of those organizations will not continue to act. Moreover, as technology advances, significant acts of terrorism may be executable by increasingly smaller terrorist infrastructures and it would thus clearly be naive to assume that small groups of people wanting to do harm to the United States will no longer be a part of America's threat environment in the future.

Since the launching of the GWOT, the State Department's Counterterrorism Office has indeed documented a reduction in the number of casualties from global terrorist attacks from 5,806 in 2001 to 3,072 in 2002, though the number subsequently increased to 4,192 in 2003.[6] Leaving aside questions relating to the problematic nature of the methodology used by the State Department in documenting terrorist attacks, it is nonetheless clear that there is no evidence to point to a trend towards significant decreases in terrorism. Admittedly it has been fewer than five years since the current campaign against terrorism was launched and thus it is difficult to predict its ultimate outcome (which is likely to be several decades away). Nevertheless, if the Pentagon proposes a strategy geared towards the destruction of terrorism, one would expect that it should have a fairly clear idea as to whether or not that outcome is achievable and what is patently obvious at present regarding the GWOT is that no individual today can reasonably predict the outcome of what American leaders, from the President on down, have consistently portrayed as a long war. Whether or not said terrorism constitutes a threat to the "American way of life" as well as the existence of a "free and open society" in the United States is unclear as these concepts are not clearly defined by the CJCS in the *NMSP*.

Since September 11, 2001, there has been only one documented domestic terrorist attack (against passengers at the El Al ticket counter at Los Angeles International Airport on July 4, 2002 carried out by a "lone wolf" terrorist with no known connections to al Qaeda) as well as a few interdictions of suspected terrorists. The overall paucity of attacks or attempted attacks would seem to suggest, given the presumably continued high motivation on the part of terrorists to attack the American homeland, that the threat of terrorism has substantially decreased within the United States. However, terrorism still constitutes a serious threat to American military personnel, American interests, and U.S. allies worldwide – and these may be considered, by some, to be important components in the process of maintaining the "American way of life." It is also possible, for example, that the current "Jihad" in Iraq is acting as a lightning-rod of sorts in drawing Salafist recruits keen on killing Americans (military and civilian) in that direction, rather than towards American shores. Of course, no one can say for sure whether the war in Iraq has actually heightened security in the American homeland or potentially decreased it, due to the radicalization of larger numbers of Muslims in Iraq and elsewhere in the wake of the U.S. invasion. At any rate, an

eventual U.S. withdrawal may free up significant numbers of Salafists for future attacks on the United States itself.

Ultimately, regardless of the situation in Iraq, there are no guarantees that the American homeland will continue to be largely free of attacks and the CIA has reportedly indicated that it considers a Chemical, Biological, Radiological, Nuclear, or high-yield Explosive (CBRNE) terrorist attack within the United States to be highly probable.[7] Additionally, with al Qaeda and its affiliates maintaining cells worldwide, increased terrorism in Europe (e.g., the Madrid and London attacks), and the strong electoral showing of Hamas in the West Bank and Gaza, extremist Shi'a factions in Iraq and the Muslim Brotherhood in Egypt, one can hardly deduce that the global environment has become substantially less hospitable to terrorists. It is also unclear as to what criteria the CJCS is using to define the term "inhospitable." If that term is taken to mean that terrorists the world over will suffer from a lack of popular support and be constantly and consistently hunted down by government security forces, then, as the aforementioned examples illustrate, this goal is far from being achieved.

Policy-makers in the Pentagon and elsewhere who desire to follow a realistic approach will be better served by not framing their counterterrorism policy in stark and unequivocal terms such as "defeat[ing] violent extremism" or creating an "inhospitable" global environment for terrorists. There is little logic in setting policy goals that are unattainable, however well-meaning they are. If one were to take a cynical approach and view the *NMSP* exclusively through the "Bureaucratic Politics" lens, one might conclude that the CJCS has drafted this strategy solely for the purpose of convincing Congress, the White House and the American people that the military needs to enjoy enhanced budgeting and greater political and operational freedom of action. Viewed in this context, the document makes sense because it suggests that the military can and will actually win the GWOT and that the military has the capabilities to operate in a wide range of contexts – traditional and non-traditional – thus both reinforcing the military's argument for increased funding and its argument for making the military the lead agency and centerpiece in the homeland security-homeland defense continuum. It would, however, require a highly suspicious mind to conclude that institutional and budgetary interests are, in fact, the main motivating factors behind the issuance of the *NMSP*. The DoD, like any other bureaucratic entity, is interested in strengthening its resources and its power relative to competing agencies. Yet there is no evidence to suggest that the Pentagon would risk putting forth a strategy of great significance for the country, based on Machiavellian considerations of narrow institutional interests. This would require assuming that leadership in DoD, from the Secretary of Defense on down, was highly selective in its form of patriotism as well as reckless. Moreover, such an approach would be extremely risky because if the true motivations were to come to light (and leaks have not been unheard of at the Pentagon), this would severely undermine the credibility, not only of the leadership at DoD, but of the entire military establishment. Finally, the *NMSP* itself points to the need for a partnership between the military and civilian agencies and hence, while putting the military in a central role, does not appear to promote a DoD monopolization

of the war on terrorism. It seems, at least to the author, that the strategy has to be taken at face value and judged based on the logic and realism of its approach.

The most critical problem, therefore, with taking an unrealistic approach to designing a counterterrorism policy is that real and effective efforts to *reduce* terrorism (as opposed to *defeating* it) may be undermined in the public perception because the overall goal of the policy has not been achieved. And it is clear that the phenomenon of terrorism is very much a public relations-focused phenomenon as both the terrorists and the government find themselves effectively waging a conflict for public opinion.[8] To the degree that the public perceives itself to be reasonably safe, the government's policies will be seen as successful. Consequently, success in countering terrorism can be measured by the degree to which the public *feels* safe from terrorism. This sense of safety has important ramifications for economic activity and other parameters by which a society may be judged capable of coping with terrorism.[9]

Clearly, the public will feel completely safe if terrorism is truly eradicated, but as this is not a realistic proposition (given the fact that disgruntled persons are a constant and technology is increasingly empowering small groups of such persons) policy-makers are best advised to find the ways and means to bolster the public perception that the government is working to enhance their security rather than promising the public something it cannot deliver. For this reason, it is also highly unlikely that the *NMSP* was drafted purely as a public relations document designed to create a popular sense of safety because if that was the primary reason behind its creation, this would represent an extremely risky and fundamentally illogical public relations strategy.

From a public relations perspective, it is preferable to provide honest and accurate information to the public – even if that information is not completely reassuring – than to paint a rosy picture that proves to be completely wrong (when the almost inevitable terrorist attacks occur) and results in the military losing its credibility in the eyes of the public. Such an outcome can only serve the terrorists by driving a wedge between the authorities and the population and encouraging mass hysteria, economic crisis and, in very extreme cases, the possible breakdown of governmental control.

One final note on this point: it is clear that only a tiny minority of Americans will ever read the *NMSP*. Therefore one might argue that promises galore may be made as no one will take the Pentagon to task for failing to achieve the goals spelled out in the *NMSP*, nor will this have much of an impact on Americans' collective sense of security. While it is undoubtedly true that the great body of Americans will remain ignorant by choice regarding specific strategies for waging the GWOT and securing the homeland, one cannot comfortably assume that the perhaps five to ten percent of Americans who have a real impact on life in the United States (prominent elected officials, economic elites, key bureaucratic players, members of the news media, the rare academic, and the occasional movie star) will remain ignorant of these strategies – particularly if they fail. Moreover, while the general public may not be particularly interested in questions of strategy, they clearly do expect the military to protect America from terrorists. If the United States falls victim to a sustained campaign of terrorism, the above groups, as well as growing numbers of the general public, are likely to perceive

the military as ineffectual and this may produce a crisis of credibility that could "trickle down" to society at large.

PROBLEM # 2: Policy Implementation Primarily Dependent on Non-DoD Entities

In order to achieve the goal of defeating terrorism in the homeland and creating a global environment inhospitable to terrorism, the CJCS suggests that the Pentagon can only succeed in this mission through cooperation with other U.S. governmental agencies (presumably also with state and local agencies, though this is not explicitly clear in the language used) and with foreign governments. The DoD is accordingly authorized to work in cooperation with other American governmental entities and foreign partners to (1) thwart or defeat terrorist actions against the U.S. and its allies, (2) attack and disrupt international terrorist networks abroad, (3) deny terrorists access to Weapons of Mass Destruction, (4) assist other countries in combating terrorism and denying terrorists safe havens in their national territory, and (5) creating a global environment inhospitable to terrorism.[10]

Some of the above missions are unclear with respect to their scope or their intention. For example, "thwart[ing] or defeat[ing] attacks against the U.S. and its allies" suggests that the Pentagon plans to militarily intervene in a wide range of terrorist "theaters of action" including many that are not directed at the United States, but rather at its allies. This would seem to imply, therefore, that the Pentagon plans to fight groups as disparate and geographically dispersed as Hamas and Palestinian Islamic Jihad, Hezbollah, the Tamil Tigers, Abu Sayyaf, the Real IRA, the followers of Shamil Basayev in Chechnya, and the like. As it is doubtful that the Department of Defense is really planning to "declare war" on disparate terrorist organizations worldwide, suggesting that this is United States policy is likely to mislead allies and create unrealistic expectations as to the scope of the GWOT as well as its targets. To provide just one example, it appears that Indo-Pakistani tensions, which almost led to the outbreak of war between the two nations in December 2001, were related to, on the one hand, India's expectation that Pakistan's support for Kashmiri separatist terrorism would put Pakistan within the camp of U.S.-defined terrorism supporters, thus bringing full U.S. support to bear behind India. On the other hand, Pakistan apparently believed that its centrality with respect to the war against the Taliban and al Qaeda meant that the United States would back Islamabad in its conflict with New Delhi.[11]

In addition to the issue of possible ally misunderstandings, should the United States fail to subsequently engage these disparate terrorist organizations, after seemingly having declared war on them, Washington will likely be viewed by international terrorists as weak, thus strengthening the belief among al Qaeda affiliates and others that the United States is not really capable of defeating global terrorism. As matters stand now, even without the possibility that the Pentagon has unwittingly created a misleading perception as to the organizations to be targeted in the GWOT, al Qaeda has been claiming that American involvement in Afghanistan and Iraq has weakened the United States irreparably (and this when the organizations targeted by the U.S. in those countries have represented a fraction of global terrorist movements).[12] Consequently, the creation of a

perception and expectation that the U.S. will fight all terrorists without exception will simply play into the hands of terrorists who, for purposes of political prestige, recruitment and the like, are working to portray the United States as weak and the GWOT as an abject failure.

Another problematic element of the strategy has to do with the commitment, outlined in the Pentagon plan, to assist other countries in fighting terrorism and preventing their national territory from being used as a safe haven for terrorists. This represents an extremely significant commitment on the part of the U.S. military. A broad range of "failed states," "failing states," or otherwise weak and misgoverned states exist in Latin America and the Caribbean, Africa and Asia. Moreover, many advanced, post-industrial states – the United States included – cannot guarantee complete control over their own homeland and are unable, with any degree of certainty, to guarantee that terrorists cannot operate from their territory. Consequently, this policy implies a profound commitment in resources (economic and military) to a large number of countries. There seems little doubt that terrorists are invariably on the lookout for failed states in which they can set up an infrastructure and the United States must clearly take this fact into account, as President Bush noted in his first *National Strategy for Homeland Security*.[13] However, building a policy around the goal of assisting states in preventing terrorists from operating in their territory is so ambitious as to be largely unrealistic. This may work to some degree in specific cases, such as with respect to the Philippines, but it is not likely to be successful on a significant scale given limited resources.[14] As in the cases of Afghanistan and Iraq, the United States military has been unable to deny terrorists the use of at least some of the territory of those countries as operational safe havens. Moreover, the cost of rebuilding Afghanistan has been estimated in the billions of dollars and the U.S. may be called upon to cover some one quarter of rebuilding costs for failed states such as Sierra Leone, Angola, Congo, Somalia, and Sudan (estimated at between $750 million and $3.75 billion over five years).[15]

Two final examples will suffice to provide a sense of the daunting task of coping with the possible security threats emanating from failed states. At present, sixteen of the eighteen United Nations peacekeeping or peace-building operations worldwide take place in failed or failing states with close to 90,000 UN personnel involved in such missions. For the present fiscal year, the cost of these missions has been estimated at $5.03 billion.[16] The United Nations, moreover, is not the only agency involved in the peacekeeping business. The West African Peacekeeping Force (ECOMOG), which has been in existence since 1990, has been deployed to Liberia, Sierra Leone and Guinea-Bissau and has been instrumental in bringing at least partial stability to these failed states – yet the cost has been high. In 2001, Nigeria, the largest contributor to the force, estimated that it has spent some $13 billion on ECOMOG since its creation.[17] It should be borne in mind, furthermore, that these international peacekeeping operations fulfill a tiny fraction of the overall need for policing and stability in a wide variety of failed states, most of which can be used, in one form or another, as effective bases for global terrorism.

Adding to the extremely problematic nature of the *National Strategy* is the fact that all of the above missions for the GWOT require significant, and in many

cases, primary, efforts to be made by non-DoD entities (whether U.S. governmental agencies at the federal, state, and local levels or foreign governments). This also makes the policy largely unrealistic because it is predicated, in essence, on the full cooperation of a broad range of American and international governmental entities. Even in the highly unlikely event that this "coalition" of entities can be assembled, there is not likely to be agreement as to which agency should take the lead (not to mention which country). Moreover, if the United States feels sufficiently threatened, it is not likely to want to encumber itself with a multilateral international response. And, for that matter, the Pentagon is likely to want to maintain control of the response and not have to share decision-making authority with other federal agencies. Take Operation Enduring Freedom, the assault on the Taliban in Afghanistan in the wake of 9/11, as an example. At European urging, NATO (invoking Article V of its founding treaty) declared that an attack on the United States was an attack on all member states, yet the United States largely bypassed the alliance in favor of what was a primarily unilateral action.[18]

Quite a number of countries are involved in different aspects of the GWOT and each operates autonomously and with its own set of interests. Pakistan and Saudi Arabia, to name just two countries, clearly have very different objectives and interests in fighting global Jihadism; to expect both to follow American priorities and interests is simply impracticable. Moreover the problem is not just an international one. Within the United States, the GWOT (in its Homeland Security context) is "fought" overwhelmingly by law enforcement entities – most of whom are local governmental entities. A host of legal and resource issues ensure that the U.S. Northern Command plays a largely marginal role in domestic counterterrorism. Beyond this, the myriad of diplomatic, informational, economic and financial counterterrorism efforts is largely not within the purview of the military, this despite the fact that the military has, through the *NMSP*, established that its policy is predicated on success in these areas as well. Consequently, by establishing the above goals as *its* policy objective, the Pentagon is putting itself in a position of weakness because it will be unable to achieve, on its own, objectives that are essentially dependent on the goodwill and cooperation of other entities, foreign and domestic.

PROBLEM #3: Countering Ideological Support for Terrorism is Not a Feasible Goal

The *National Military Strategy* puts much emphasis on its assertion that ideological support for terrorism constitute the enemy's "strategic center of gravity," and that the military can help undermine such support through: (1) creating a secure environment for political moderates (presumably in countries where such moderates face intimidation in the face of support for terrorists), (2) demonstrating goodwill through humanitarian assistance, (3) strengthening military-to-military contacts in order to influence foreign leaders in their counterterrorism policies, (4) conducting operations abroad in a manner that does not offend the sensibilities of foreigners, and (5) strengthening the voices of moderates abroad through information operations.[19]

While the document does acknowledge that the military is not likely to be the lead agency in this area, it nevertheless sets goals, in partnership with other federal agencies, that will be difficult, if not impossible, to meet. Most students of terrorism acknowledge that in order for terrorism to be effective, it requires a minimal base of popular backing in the form of passive and active cadres of supporters or, using the systems analysis model, a series of mutually interdependent concentric rings moving from the hard-core leadership to various levels of sympathizers fulfilling a myriad of support and infrastructure functions.[20] It is therefore clear that terrorists will have a significantly more difficult time operating in a hostile public environment and a number of cases have shown that terrorist groups will sometimes change tactics when faced with a possible significant drop in support among traditional groups of supporters.[21] Consequently, the goal of encouraging political moderates in countries in which terrorists derive popular support is unquestionably praiseworthy. The problem is that it is not clear how this will be accomplished and whether the Pentagon, in cooperation with or independent of other federal agencies, possesses the wherewithal to achieve this objective.

The creation of a secure environment for moderates throughout the Middle East, to take what is perhaps the most problematic region in this context as an example, requires a mind-boggling investment in resources and manpower. Among the many measures that such a policy is likely to require are: (1) the provision of significant military forces to maintain law and order in the absence of the ability and/or willingness of the host country to provide a physically safe environment for moderates (something that does not exist in Iraq today despite the current deployment of some 150,000 U.S. troops in that country), (2) the revamping of educational systems in most Middle East countries in a manner that will encourage the teaching of moderation and democratic principles and eschew time-honored religious and societal values, (3) the creation of democratic political systems that encourage political moderation and moderate debate, and (4) the creation of a significant upwardly-mobile middle class that can act as a repository of moderation and democratic values. In short, the task is daunting to say the least – so daunting in fact, as to be wholly quixotic. Moreover, such a policy would clash with the fourth policy goal: conducting foreign operations in a manner that is politically, socially, and culturally acceptable to the target populations. The deployment of significant numbers of U.S. troops in order to provide security for political moderates is not likely to endear the United States to those target populations and not likely to foster credibility for the kind of moderate and democratic values that the policy aims to encourage and solidify. Similarly, the creation of U.S.-funded, or at least U.S.-vetted, educational systems is highly likely to be seen (given the current environment of mistrust, if not outright hostility, towards the United States) as a form of American "cultural imperialism" and consequently has a very low probability of success.

The *National Strategy* also suffers from inherent contradictions in that, on the one hand, it tasks the military (albeit in cooperation with other federal agencies) with the job of creating a supportive environment for moderates in the Islamic world and yet, on the other hand, recognizes that support for moderation and the eschewing of violence and terrorism must come from the Muslim inhabitants of

these countries. The Islamic world is expected to "*progressively recognize*... [that] violent extremist actions... [are]...a threat to itself through *introspection*" (emphasis added).[22] It is not clear whether the *National Strategy* envisions that *introspection* to come about as a result of introducing U.S. "boots on the ground" in those countries (in order to provide security to moderates and thus foster a climate of debate and introspection) or whether it will come about through active hostilities that will cause sufficient hardship to Muslims that they will realize the "error of their ways" and, through *introspection*, reach the conclusion that the path of moderation is best.

It thus appears that the "bottom line" of the CJCS's *National Military Strategy for the War on Terrorism* is that the success of U.S. counterterrorism policy is dependent on the willingness of the Islamic world to overcome the powerful attraction of Salafist Islam. By essentially suggesting this, the Pentagon has absolved itself of ultimate responsibility for effectively fighting terrorism as the military is not likely to be a successful agent for change at the grassroots level in the Islamic world. Yet at the same time, the CJCS has set the initiation of this change, and the subsequent expected reduction in, or eradication of, terrorism as a central policy goal for the military.

LIMITING GOALS TO ACHIEVE RESULTS

The *NMSP*'s primary flaw is that it sets out policy goals that are highly impractical and ultimately largely unachievable.[†] In so doing, it will not only embolden America's enemies when the United States invariably fails to achieve those policy goals, but also will create unrealistic expectations among allies and the American public (or at least the more prominent segments within it). The danger here is that not meeting those expectations will create a sense that the government and military are losing the war on terrorism because central policy goals set out by the military are not being met. Furthermore, due to the highly psychological nature of terrorism, if Americans become convinced that the United States is losing the war on terrorism, the United States will, in effect, have lost. Even in the case of conventional wars, public sentiment can play a crucial role (many historians point to the fact that the U.S. lost the Vietnam War in the court of public opinion and not on the battlefield). What is true for a conventional war is true even more so for the Global War on Terrorism.

[†] While one might argue that the goals set out in the *NMSP* do not have to be achieved simultaneously and therefore some of the objectives may meaningfully be addressed first and others later, a closer look at the strategy shows that progress in one area is dependent on parallel progress in other areas. The *NMSP* in fact refers to elements of the strategy being buttressed by "cross-cutting enablers" (i.e., factors that affect all of the components of the strategy). For example, attacking terrorists abroad, one of the components of the strategy, requires expanding foreign partnerships, strengthening capacity to prevent terrorist acquisition of CBRNE, and institutionalizing international strategies against terrorism – all of these being cross-cutting enablers. Consequently, the policy being proposed resembles a matrix in which forward movement requires advancement both in the components of policy and in the so-called cross-cutting enablers. This, in fact, largely precludes the option of focusing first on only a few components of the policy and then moving forward on others.

Some may argue that the DoD should purposefully set out goals that are more "aspirational" in nature – in other words, goals that one does not expect realistically to achieve, but that outline the vision and direction policy should take. It is intuitive that policymaking without vision lacks coherence and cohesion. Viewed within this rubric, the *NMSP* might not be seen as quite so problematic. However, the need for vision does not mean that all policy documents at all levels should incorporate so-called aspirational goals. In this instance, the vision for defeating global terrorism would probably best be expressed at the White House/NSC level (rather than at the level of those who are more frequently tasked with implementing policy) and when it is expressed by the president, should be clearly labeled as "aspirational," "long term," "visionary," and the like, so as not to create the impression that is within the country's immediate grasp.

Given the above, in order to develop a credible and realistic strategy for dealing with terrorism, the military should play to its strengths and comparative advantages. The military establishment's primary role is to apply physical power in order to achieve national objectives. In this case, this means that the military focuses on the physical disruption of terrorist networks and the apprehension or liquidation of individual terrorists. The *NMSP* correctly spells out these goals and notes that they are a major part of the military's mission, but then it goes into unfamiliar territory, for the military, by dealing with overtly non-military issues as well as ones in which the DoD subordinates itself to other domestic agencies and/or foreign countries. The American public can legitimately and realistically expect the military to be competent and effective (though not necessarily successful 100% of the time) in counterterrorist efforts within the purely military sphere. Why, then, should the Pentagon willingly embrace "mission creep" and dive head-and-shoulders into complex and muddled economic, financial, cultural, educational, etc. issues that relate to broader societies? The military is infinitely more prepared and competent to arrest or kill terrorists and destroy their bases than it is to change values, societal structures, and political regimes. It is immeasurably better to produce a successful limited policy than a failed all-encompassing one. As with any illness, it is always better to treat the root causes, but some diseases are presently incurable and the best way to manage them is by addressing their symptoms.

The Pentagon should also understand that it cannot stand aside and put the impetus for change on others – particularly societies that are not predisposed to view the United States, or Western values and culture in general, in a positive light. If the success of the military's counterterrorism efforts is dependent on fundamental change being initiated by Muslims from within the Islamic world, then the military has willingly abrogated its control of the situation and virtually ensured that its policy (barring any sudden, dramatic democratization of the Islamic world – something which is a distinctly unlikely eventuality) will be seen as a failure. This will ultimately create serious misgivings within American society and produce the opposite of what the military is trying to achieve. Instead of strengthening America's security (through creating a strong public *sense of security*) the military will have unwittingly contributed to undermining that security.

In sum, the *National Military Strategy for the War on Terrorism* should be just that: a *military* strategy, not a political, economic, or social one. The argument presented here does not suggest that the elements of "Soft Power" referred to in the *NMSP* (such as economic, cultural, educational, and attitudinal issues) do not need to be addressed or that they are not desirable components (allowing for the fact that some are more aspirational in nature and others more concrete) of an overarching counterterrorism policy. Rather, the author takes issue with the military taking "ownership" of this strategy because the military is far more qualified to address the elements of "Hard Power" (in this case, attacking terrorist bases overseas and the regimes that harbor them) than it is in addressing these other issues.

Whether Americans and other Westerners care to admit this or not, Jihadist terrorism is likely to be a reality for some time to come and there is probably little the United States can do to fundamentally alter the status quo in the lslamic world. The U.S. military can, however, fight terrorists in the traditional sense of the term. By setting this as its true policy goal, the Pentagon will be creating a goal that is achievable. "Fighting" does not imply always "winning," but ultimately the American public will be more reassured when they see a limited and realistic policy pursued rather than seeing their military touting a military *cum*-political-economic-cultural-educational panacea that is highly likely to be an unmitigated failure.

Nadav Morag *is a faculty member at the Center for Homeland Defense and Security (CHDS) at the Naval Postgraduate School in Monterey, California and holds positions as associate professor and chair of the Department of Political Science at the University of Judaism in Los Angeles, as well as a senior research consultant at the university's Center for Israel Studies. He also serves as a member of the Los Angeles County and Orange County Sheriff's Departments' Homeland Security Advisory Council and is a member of the Los Angeles County Terrorism Early Warning Group. Dr. Morag received his bachelor and master degrees from UCLA and his Ph.D. from Tel Aviv University, where he also taught for nine years.*

---

[1] Department of Defense, *Strategy for Homeland Defense and Civil Support* (Washington, D.C.: Department of Defense, 2005), 11-13.

[2] Office of Homeland Security, *The National Strategy for Homeland Security* (Washington, D.C.: Office of Homeland Security, 2002), vii.

[3] Department of Defense, *Strategy for Homeland Defense and Civil Support*, 14.

[4] Richard B. Meyers, *National Military Strategic Plan for the War on Terrorism* (Washington, D.C.: Joint Chiefs of Staff, 2006), 5.

[5] Ian Bruce, "MI5 Told to Use More Resources on IRA Groups," *The Herald*, May 23, 2006 http://www.theherald.co.uk/news/62510.html.

[6] United States Department of State, Office of the Coordinator for Counterterrorism, *Patterns of Global Terrorism 2003* (Washington, D.C.: Department of State, 2004) http://www.state.gov/s/ct/rls/pgtrpt/2003/33777.htm.

[7] "Al-Qaeda and the Bomb," *Jane's Intelligence Digest*, July 3, 2003.

[8] See Paul Wilkinson, *Terrorism and the Liberal State* (New York: New York University Press, 1970), 110-114; Walter Laqueur, *The New Terrorism: Fanaticism and the Arms of Mass Destruction* (Oxford:

Oxford University Press), 43-44; Bruce Hoffman, *Inside Terrorism* (New York: Columbia University Press, 1998), 131-136.

[9] See Nadav Morag, "Measuring Success in Coping with Terrorism: The Israeli Case," *Studies in Conflict and Terrorism*, Vol. 28, no. 4 (July/August 2005),and Nadav Morag, "The Economic and Social Effects of Intensive Terrorism: Israel 2000-2004," *Middle East Review of International Affairs* (forthcoming).

[10] Meyers, *National Military Strategic Plan*, 6.

[11]Polly Nayak, *Reducing Collateral Damage to Indo-Pakistani Relations from the War on Terrorism*, Policy Brief #107 (Washington, D.C.: The Brookings Institution, 2002), 2-3 http://www.brookings.edu/comm/policybriefs/pb107.pdf.

[12] Radio Free Europe/ Radio Liberty, "Middle East: Al-Qaeda Tape Says US Losing in Afghanistan, Iraq," September 10, 2004. http://www.rferl.org/features/features_Article.aspx?m=09&y=2004&id=724B42FC-3872-4D9C-B7CC-9529864F6419.

[13] George W. Bush, *National Strategy for Homeland Security* (Washington, D.C.: Office for Homeland Security, 2002), 10. http://www.dhs.gov/interweb/assetlibrary/nat_strat_hls.pdf.

[14] United States Department of State, Office of the Coordinator for Counterterrorism, *Country Reports on Terrorism 2005* (Washington, D.C.: Department of State, 2006), 77-80. http://www.state.gov/documents/organization/65462.pdf.

[15] Susan E. Rice, *The New National Security Strategy: Focus on Failed States*, Policy Brief # 116 (Washington, D.C.: The Brookings Institution, 2003), 7. http://www.brookings.edu/comm/policybriefs/pb116.pdf.

[16] United Nations, *United Nations Peacekeeping Operations. Background Note 28* (New York: United Nations Department of Public Information, 2006) http://www.un.org/depts/dpko/dpko/bnote.htm.

[17] BBC News, "Profile, ECOMOG," June 17, 2004. http://news.bbc.co.uk/2/hi/africa/country_profiles/2364029.stm.

[18] Wesley Clark, "An Army of One? In the War on Terrorism, Alliances are not an Obstacle to Victory. They are the Key to it," *Washington Monthly* (September 2002). http://www.washingtonmonthly.com/features/2001/0209.clark.html.

[19] Meyers, *National Military Strategic Plan,* 7-8.

[20] Mark S. McAlpine, "Future Roles of Air and Space Power in Combating Terrorism" (research paper, Air Command and Staff College, 1997), 11-12. http://www.maxwell.af.mil/au/awc/awcgate/acsc/97-0393.pdf

[21] Anat Kurtz, "Non-Conventional Terrorism: Availability and Motivation," *Strategic Assessment* 7, no. 4 (March 2005). http://www.tau.ac.il/jcss/sa/v7n4p6Kurz.html

[22] Meyers, *National Military Strategic Plan,* 20.

Social Network Analysis as an Approach to Combat Terrorism: Past, Present, and Future Research

Steve Ressler

INTRODUCTION

The greatest security threat facing the United States is not from formal states, but from terrorist organizations that attack informally, using terror at any time and place, with the goal of undermining confidence in U.S. institutions and the American way of life. No longer a structured battle that can be fought with military power, the war against terrorism will be won with superior knowledge.

Due to the changing nature of homeland security issues, a new type of intelligence is needed by homeland security: social network analysis (SNA). The basis of social network analysis (also known as network science or network sociology) is that individual nodes (which, depending on the type of network, can be people, events, etc.) are connected by complex yet understandable relationships that form networks.[1] These networks are ubiquitous, with an underlying order and simple laws. Networks form the structural basis of many natural events, organizations, and social processes.

Terrorist organizations are well-suited to study using social network analysis, as they consist of networks of individuals that span countries, continents, and economic status, and form around specific ideology. Terrorist organizations are different from hierarchical, state-sponsored appointments in characteristics such as leadership and organizational structure. Social network analysis can provide important information on the unique characteristics of terrorist organizations, ranging from issues of network recruitment, network evolution, and the diffusion of radical ideas. Specifically, social network analysis can be used to understand terrorist networks, inform U.S. homeland security policy, and form the basis of a more effective counter-measure to net war.

SOCIAL NETWORK ANALYSIS

The origin of contemporary social network analysis can be traced back to the work of Stanley Milgram.[2] In his famous 1967 experiment, Milgram conducted a test to understand how people are connected to others by asking random people to forward a package to any of their acquaintances who they thought might be able to reach the specific target individual.[3] In his research, Milgram found that most people were connected by six acquaintances. This research led to the famous phrase “six degrees of separation,” which is still widely used in popular culture.

Another important step in the development of social network analysis was the work of Mark Granovetter on network structures. In his widely-cited 1973 article “The Strength of Weak Ties,” Granovetter argues that “weak ties” – your relationships with acquaintances – are more important than “strong ties” – your relationships with family and close friends – when trying to find employment.[4] Granovetter's article and subsequent research extended this argument by positing that more disperse, non-redundant, open networks have greater access to information and power than smaller,

denser, and more interconnected networks because they supply more diversity of knowledge and information.

D.J. Watts' small world hypothesis builds upon both Milgram's "six degrees of separation" concept and Granovetter's "weak ties" argument by stating that most networks in the natural and man-made world are highly clustered yet far-reaching.[5] These networks have a "clustered" center, where most nodes are neighbors, tightly interconnected. In addition, each has weak ties that can connect it to any node in the network in a few short connections. For example, if a node represents a person, a person's friendship network is generally tightly connected, with common friends, similar backgrounds, and overlaps. However, despite this "clustered" inner core, as shown with Milgram's "six degrees of separation," a person can reach a stranger in the world through only a few small steps/connections. Watts' small world argument has been extended by numerous researchers to help understand the structure and behavior of various networks, including the spread of AIDS, the collapse of financial markets, and the spread of information.[6]

The value of social network theory versus other political science and sociological approaches is its focus on the value of the network structure rather than the characteristics of the individual. While social network analysis leaves room for individuals to affect their fate, it argues that the structure of the network and relationships and ties with others in the network are more important. The network structure of an organization (in this case a terrorist organization) will affect its ability to access new ideas, recruit new individuals, and achieve sustainability. Network analysis seems to work because it provides a structural analysis while still leaving room for individual effort. In a sense, network analysis builds upon many organizational theories, since networks are just another organizational structure. As Charles Perrow discusses in his work *Complex Organizations*, many organizational theories have evolved over time in an attempt to explain the organization structures of the related era.[7] Network structure is a modern organizational structure, whose power may be built upon the idea of disintermediation. Disintermediation is the removal of the intermediary role in a process or supply chain, a proverbial "cutting out the middleman." Modern social networks are building upon this idea of disintermediation as individuals can directly connect to each other especially with the advancements of modern telecommunications and the Internet. The power of loosely structured networks is that they can move quickly and be adaptive, as they do not need to go through layers of a hierarchical chain. Disintermediation is important for terrorist networks as they have cut out layers of bureaucracy; individuals can join a network through weak ties and plan attacks through loose connections.

While social network analysis has been present in some form for decades, the concept entered popular culture in the beginning of the twenty-first century. Malcolm Gladwell's bestseller *The Tipping Point* uses basic network ideology to describe how real-world social epidemics occur, such as the popularity of Airwalk shoes and the decline of crime in New York City.[8] Gladwell describes the importance of three types of people: connectors, mavens, and salesman. Gladwell builds upon Watts' research as he describes connectors – those with wide social circles – as the hubs of the human social network and responsible for the small world phenomenon.

The use of social network analysis in the mainstream has increased with the growth of a number of new online Internet sites based on social network principles. For

example, MySpace, Friendster, and Facebook are three websites that allow users to connect with friends and friends of friends to share photos, blogs, user profiles, and messages. Especially important in teenager culture, these sites map out each user's network of friends and acquaintances. According to Alexa.com, a web trafficking service, as of April 2006, MySpace is the third most popular website in the U.S. and the sixth most popular in the world ("Top 500 Sites"). Further, similar websites have been created in the employment field. Sites such as LinkedIn allow members to map their professional connections and allow employers and employees to use their associations as references in job matching.

SOCIAL NETWORK ANALYSIS AND TERRORISM

The importance of SNA in fighting the war on terrorism was recognized even before the attacks of September 11, 2001. John Arquilla and David Ronfeldt's work *Networks and Netwars,* which was released in 2001 before the terrorist attacks, describes the increased network principles in modern criminal organizations.[9] The premise of the book is that war is no longer a head-to-head battle of two powers. There is no formal hierarchical-based enemy like the U.S.S.R. during the Cold War. Modern war is *netwar*, a lower-intensity battle by terrorists, criminals, and extremists with a networked organizational structure. These networked structures are often leaderless and able to attack more quickly. Novel, asymmetric approaches are needed to combat a network-based criminal organization.

After the attacks of 9/11, academia, the government, and even mainstream media began to discuss the importance of social network analysis in fighting terrorism. Mainstream media outlets such as the *Washington Post* and the *Dallas Morning News* ran articles describing the potential benefits of network science.[10] Authors of popular press network books, such as Antonio-Laszlo Barabasi (*Linked*), were interviewed extensively, on television and radio programs, on how we could use the knowledge of social networks to fight terrorism. Further, when the National Security Agency's warrant-less eavesdropping program hit the news in 2006, the importance of social network analysis in fighting terrorism reemerged in a *New York Times* article discussing the ability of network analysis to map and potentially make meaning out of the millions of communications NSA intercepts daily between individuals.[11]

Academic Activities

After 9/11, social network experts in academia began to look explicitly at the use of network methodology in understanding and countering terrorism. The listserv associated with the leading social network organization, International Network for Social Network Analysis (INSNA), was inundated with questions, comments, and concerns over the role of social network analysis in the fight against terrorism. In the winter of 2001, *Connections*, the social network journal affiliated with INSNA, devoted an issue to social network analysis and terrorism. In this issue, Valdis Krebs begins to map the Al-Qaeda network by collecting public available data on the Al-Qaeda hijackers and running basic network principles through computer software.[12] The rest of the articles in this issue are more or less data-free. Kathleen Carley and others describe the potential uses of social network analysis and multi-agent modeling to destabilize

terrorist networks.[13] Richard Rothenberg conjectures on the structure of the al Qaeda terrorist network based on newspaper articles and radio commentary.[14]

Since the winter of 2001, the academic world has increased the attention paid to the social network analysis of terrorism as a result of public interest and new grant money.[15] Network analysis of terrorist organizations continues to grow and can be divided into two groups: the data collectors and the modelers.

Data Collectors

Data collection is difficult for any network analysis because it is hard to create a complete network. It is especially difficult to gain information on terrorist networks. Terrorist organizations do not provide information on their members, and the government rarely allows researchers to use their intelligence data. A number of academic researchers focus primarily on data collection on terrorist organizations, analyzing the information through description and straightforward modeling. Valdis Krebs was one of the first to collect data using public sources with his 2001 article in *Connections*. In this work, Krebs creates a pictorial representation of the al Qaeda network responsible for 9/11 that shows the many ties between the hijackers of the four airplanes. After the Madrid bombing in 2004, Spanish sociologist Jose A. Rodriguez completed an analysis similar to Krebs' by using public sources to map the March 11th terrorist network. In his research, he found diffuse networks based on weak ties amongst the terrorists.[16]

Another bright spot is the 2004 publication of *Understanding Terror Networks* by Marc Sageman. Using public sources, Sageman collects biographies of 172 Islamic terrorist operatives affiliated with the global Salafi jihad (the violent revivalist Islamic movement led by al Qaeda). He uses social network analysis specifically on Al Qaeda operatives since 1998. This analysis yields four large terrorist clusters. The first cluster resides in the Pakistan-Afghan border and consists of the central staff of al Qaeda and the global Salafist jihad movement. The second cluster is a group of operatives located in core Arab states such as Saudi Arabia, Egypt, Yemen, and Kuwait. The third cluster is known as the Maghreb Arabs who, although they come from North African nations, currently reside in France and England. The final cluster is centered in Indonesia and Malaysia and is affiliated with Jemaah Islamiyah.[17]

Despite their many strengths, Krebs' and Sageman's works have a few key drawbacks. By dealing with open sources, these authors are limited in acquiring data. With open sources, if the author does not have information on terrorists, he or she assumes they do not exist. This can be quite problematic as the data analysis may be misleading. If one cannot find an al Qaeda operative in the U.S. in publicly available sources, the researcher could assume there is no al Qaeda network. However, it is highly probable this is not the case, since terrorists generally try to keep a low profile before committing an attack. The data collectors can also be criticized because their work is more descriptive and lacks complex modeling tools. Fostering relationships with modelers could augment the work being conducted by data collectors, as statistical analysis might be able to take into account some of the limitations of the data and provide an additional analytical framework.

One promising activity is the development of a major terrorism web portal at the University of Arizona's Artificial Intelligence Center. This website makes social network tools and data related to terrorism publicly available.[18] One example is the Terrorism

Knowledge Portal, a database consisting of over 360,000 terrorism news articles and related Web pages coming from various high-quality terrorism Web sites, major search engines, and news portals. By providing publicly available network tools and data, the research opens itself to a number of new scholars. Academics can double-check the work of others to ensure quality. New scholars can enter the field without the lengthy time commitment and financial cost of developing basic tools and getting data. Such activities, combined with the federal government's support, will help push the field of terrorism-related social network analysis to new heights in the future.

Modelers

Complex models have been created that offer insight on theoretical terrorist networks. Kathleen Carley heads one of the largest computational model organizations that models terrorist networks, Computational Analysis of Social and Organizational Systems (CASOS) at Carnegie Mellon University. Carley, along with her team of faculty and graduate students, has a number of ongoing projects in the Networks and Terrorism division that have received funding from government sources ranging from the Office of Naval Research to the Department of Defense. In a series of projects, Carley and her collaborators deal with a variety of terrorism-related issues. They looked at how to model the shape of a covert network when little information is known, through predictive modeling techniques based on inherent network structures.[19] Using a computational tool created at CASOS known as DyNet, they looked at ways to estimate vulnerabilities and destabilize terrorist networks.[20] They also developed a city-level network model of chemical and biological attacks (BioWar) in an attempt to understand how people move in networks that affect what they know, what they do, how they respond, especially when they get diseases, how they get diseases, and how they react.[21] Finally, they use network text analysis, a method used to define and model the relationships between words in a text, to turn raw text related to Mideast covert networks into a pictorial network representation of the social and organizational structure of a covert network.[22] Besides the aforementioned work, Carley and her team are beginning to look at a range of other related issues including work on the effectiveness of wiretapping programs in mapping the networks of rapidly evolving covert organizations.[23]

There has been limited work in the field of complex modeling of terrorist networks outside the work of Kathleen Carley and her associates. One group using complex models to look at terrorism issues is the researchers at the University of Arizona Dark Web Terrorism Research Center. In a series of articles, researchers at this center published a number of articles in which they used social network tools to study extremist-group web forums.[24] Through the analysis of web forum activities, they were able to construct social network maps and organization structures. In addition, in 2002, Tami Carpenter and others began to look at some of the practical issues and algorithms for analyzing terrorist networks by discussing a number of ways to construct various social network measures when dealing with covert networks.[25] Besides the aforementioned works, a few of the major social network analysis scholars such as Steve Borgatti at Boston College and David Jensen at University of Massachusetts have discussed the general implications of social network analysis of terrorist networks in invited presentation and conference talks; but they have not undertaken the issue in detail with complex modeling.

A common problem for the modelers is the issue of data. Any academic work is only as good as the data, no matter the type of advanced methods used. Modelers often do not have the best data, as they have not collected individual biographies (like Sageman) and do not have access to classified data. Many of the models are created data-free or without complete data, yet do not fully consider human and data limitations. The implication of this is that the results can be potentially misleading, as they cannot take into account behavioral and contextual issues that might affect the network structure and activity. For example, it would be quite difficult to model the network structure and evolution of al Qaeda since many of the organizations that claim ties to al Qaeda are lying and do not actually have those ties. It can be quite difficult differentiating these groups from other, truly loosely affiliated groups.

In addition, modelers often do not have a foundation in terrorist studies nor do they always work with top counter-terrorism experts. Without the help of counter-terrorism experts or a background in terrorism studies, it is difficult to turn the numbers and graphic models into interpretable results that make sense in the context of the vast literature on terrorism. The vast body of knowledge in terrorism studies created since the 1970s can provide a context for the network data created by the modelers, including the historical and political trends exhibited in terrorism, reasons people join terrorist groups, and the psychology of terrorist attack tactics, including suicide terrorism.[26]

Government Activities

Despite the seeming novelty of social network analysis, the federal government has used link analysis, a predecessor of SNA, for nearly fifty years. Karl Van Meter describes the two main types of link analysis: the village survey method and traffic analysis.[27] The village survey method was created and used by Ralph McGehee of the CIA in Thailand in the 1960s to understand family and community relationships. He conducted a series of open-ended interviews and in a short time was able to map out the clandestine structure of local and regional Communist organizations and associated "sympathetic" groups. Traffic analysis (also known as communication link analysis) began during World War II and its importance continues to this day. This technique consists of the study of the external characteristics of communication in order to get information about the organization of the communication system. It is not concerned with the content of phone calls, but is interested in who calls whom and the network members, messengers, and gatekeepers. Traffic analysis was used by the British MI5 internal security service to combat the IRA in the 1980s and 1990s and continues to be used across the world by law-enforcement agencies including the U.S. Defense Intelligence Agency (DIA) Office of National Drug Control Policy.[28]

The *Analyst Notebook* is the primary software used for link analysis. Currently on its sixth version, this software is recognized as one of the world's leading analytical tools and is employed in more than 1,500 organizations ("Contraband Enforcement"). Social network analysis improves upon link analysis by moving from single variable analysis to multivariate analysis, allowing the individual to control for many factors at once. The change from single variable to multivariate analysis is quite significant when researching terrorism: a number of factors affect terrorism, not one single factor. For example, the propensity for one to participate in a terrorist activity might not be strongly affected by the single variable of being related to a terrorist member. However, the combination of multiple variables such as poverty, type of government, combined

with the link to a terrorist member may cause a person to participate in a terrorist activity. Multivariate analysis allows us to take into account these multiple variables and their effects when controlling for another variable.

From the outside, it is difficult to understand how social network analysis is being used in the federal government. Confidentiality prevents government social network analysts from discussing their work with professors and private companies without security clearances. Despite this lack of information, it is clear that the federal government is interested in using network techniques in fighting the war on terror. Many government agencies, such as the Defense Advanced Research Projects Agency (DARPA), U.S. Army Research Labs, the U.S. Office of Naval Research (ONR), the National Security Agency (NSA), the National Science Foundation (NSF) and the Department of Homeland Security (DHS), have funded research related to social network analysis. Also in the past few years, government agencies such as the Navy Joint Warfare Committee have created openings for network analysts. DHS has instituted the Department of Homeland Security Graduate Fellowship program for graduate students interested in terrorist-related studies. This program has funded research specifically in the field of network analysis. However, aside from these activities, the number of government employees actually using network analysis is unclear. The best evidence in this regard is the admission, by the few known government social network analysts, that social network techniques are quite prevalent but they will not discuss the specifics of this approach's use in government anti-terrorist activities.

DISCUSSION

The main limitation of social network analysis is the same that applies to any new and innovative technology: social network analysis is just one tool that can be used to understand terrorism, and is just one piece of the puzzle. Subject matter experts are needed to provide a context for the research. Furthermore, the basic assumption of network analysis regarding terrorism may not be completely valid. Despite their non-hierarchical approach, terrorist organizations are not completely organized in a network structure. There are still central headquarters and training facilities for most terrorist organizations. Also, social network analysis must attempt to address the underlying root cause of terrorism. It is helpful to understand how a network evolves and how to destabilize a network. It is more helpful, however, to understand how networks recruit participants and why people wish to join terrorist networks.

I would like to see an expansion of the research areas in which network analysis is being used with regard to terrorism. Only a limited amount of work has been completed, and there is much room for this tool to yield great insights into terrorism. I would be particularly interested to see this method used to analyze network recruitment. Network analysis could identify recruiters from peripheral participants, as well as the demographic and personal characteristics that repel – as well as draw – an individual to a terrorist organization. Are terrorist recruiters generally introduced to the organization through weak ties or strong ties? These characteristics may also affect the individual's degree of participation in terrorist activity. Such research could potentially help intelligence analysts in creating strategies to counteract terrorist recruiting initiatives.

Network analysis can also be used to understand the psychological effect of terrorism. One of the main effects of terrorism is fear, which is spread through network

structures such as media, the Internet, and personal relationships. For example, the number of ties an individual has to victims of terrorism may impact the individual's perception of the risk of terrorism. Finally, I would like to see further research on network structure evolution. It would be interesting to compare the structure of multiple terrorist networks to see how they evolve over time. The network structure may impact the ability of an organization to endure over the years and complete attacks. It is important for intelligence analysts to understand how to break up a network; they could potentially exploit the small world topology by eliminating weak ties in order to isolate the network and diminish its reach and power. The removal of individuals in key network locations may be even more important than attacking the traditional leaders of a group.

Further, I hope to see an expanded use of social network analysis among homeland security educators and practitioners. Homeland security education is in a pre-paradigm phase as a professional discipline and is being conceptualized differently among educators. Christopher Bellavita and Ellen Gordon have identified over fifty topic areas related to homeland security education; I would like social network analysis to be taught as one of the tools available in a number of these areas, including risk management and analysis, intelligence, terrorism prevention, and the sociology of homeland security.[29] Further, I would like to see increased use of social network analysis by intelligence analysts. As Bellavita has pointed out, the U.S. suffers from the fear of imagination when it focuses on the idea of prevention and we need new tools.[30] It is difficult for a hierarchical organization to cope with a widely dispersed, loosely integrated, disintermediated adversary; the U.S. government may want to consider changing some of its organizational structures to effectively fight such a foe. It may be worth experimenting with pilot programs in the intelligence community that consist of decentralized, loose networks of government employees, spanning the globe with various jobs and ideas, but focused on one goal: stopping terrorists.

The author would like to thank the Department of Homeland Security Scholars and Fellows Program for support of this research and ANSER for their help supporting this research while he was an intern there. Further, he would like to thank Laurence Raine, Joshua Sinai, and Elizabeth Vaquera for their help reading earlier drafts of this research paper.

Steve Ressler *is a member of the first class of the Department of Homeland Security Graduate Fellowship Program and president of the DHS Scholars and Fellows Alumni Program. He received his master's degree in sociology at the University of Pennsylvania, where he conducted research on social network analysis. He completed this article while a DHS Fellow intern at the ANSER Homeland Security Institute. Currently, Mr. Ressler serves as an IT auditor for the Department of Homeland Security.*

Suggested Web Links

http://www.insna.org (International Network for Social Network Analysis)
http://www.orgnet.com (Valdis Krebs' web page on social network analysis)
http://ai.bpa.arizona.edu (University of Arizona's Artificial Intelligence Center)
http://www.casos.cs.cmu.edu (Computational Analysis of Social and Organizational Systems (CASOS) at Carnegie Mellon University)

[1] Albert-Lazlo Barabasi, *Linked: The New Science of Networks* (New York: Perseus, 2002).
[2] Linton Freeman, *The Development of Social Network Analysis: A Study in the Sociology of Science* (Vancouver: Empirical Press, 2004).
[3] Stanley Milgram, "The Small World Problem," *Psychology Today,* May 1967: 60-67.
[4] Mark Granovetter, "The Strength of Weak Ties," *American Journal of Sociology* 78, no. 6 (1973): 1360-1380.
[5] D.J. Watts, "Networks, dynamics and the small world phenomenon," *American Journal of Sociology* 105, no. 2 (1999): 493-527.
[6] Mark Buchanan, *Small Worlds and the Groundbreaking Science of Networks* (New York: W.W. Norton, 2002).

[7] Charles Perrow, *Complex Organizations: A Critical Essay* (New York: Random House, 1986).
[8] Malcolm Gladwell, *The Tipping Point* (New York: Little Brown, 2000).
[9] John Arquilla and David Ronfeldt, eds. *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Washington, D.C.: RAND, 2001).
[10] J. Garreau, "Disconnect the Dots," *Washington Post,* September 17, 2001; Tom Siegfried, "Network Science Could Provide Patriotic Gains," *Dallas Morning News,* September 9, 2002.
[11] Patrick Keefe, "Can Network Theory Thwart Terrorists?" *New York Times,* March 12, 2006.
[12] Valdis Krebs, "Mapping Networks of Terrorist Cells," *Connections* 24, no. 3 (2001): 43-52.
[13] Kathleen Carley, Ju-Sung Lee, and David Krackhardt, "Destabilizing Terrorist Networks," *Connections* 24, no. 3 (2001): 79-92.
[14] Richard Rothenberg, "From whole cloth: making up the terrorist network," *Connections* 24, no. 3 (2001): 36-42.
[15] See, for example, A. Abbasi and H. Chen, "Identification and Comparison of Extremist-Group Web Forum Messages using Authorship Analysis," *IEEE Intelligent Systems* 20, no. 5 (2005); Kathleen Carley, M. Dombroski, M. Tsvetovat, J. Reminga and N. Kamneva, "Destabilizing Dynamic Covert Networks," in *Proceedings of the 8th International Command and Control Research and Technology Symposium* (Washington, D.C.: War College, 2003); Kathleen Carley, Neal Altman, Boris Kaminsky, Démain Nave and Alex Yahja, "BioWar: A City-Scale Multi-Agent Network Model of Weaponized Biological Attacks," CASOS Technical Report, CMU-ISRI-04-101 (2004); J.A. Rodriquez, "The March 11th Terrorist Network: In its weakness lies its strength," XXV International Sunbelt Conference, Los Angeles, 2005; and Y. Zhou, E. Reid, J. Qin, G. Lai, and H. Chen, "U.S. Domestic Extremist Groups on the Web: Link and Content Analysis," *IEEE Intelligent Systems* (Special issues on artificial intelligence for national and homeland security, forthcoming).
[16] Rodriquez, "The March 11th Terrorist Network."
[17] Marc Sageman, *Understanding Terror Networks* (Philadelphia: University of Pennsylvania Press, 2004).
[18] Edna Reid, Jialun Quin, Wingyan Chung, Jennifer Xu, Yilu Zhou, Rob Schumaker, Marc Sageman, and Hsinchun Chen, "Terrorism Knowledge Discovery Project: A Knowledge Discovery Approach to Address the Threats of Terrorism," (Working paper, 2004).
[19] Matthew Dombroski, Paul Fischbeck, and Kathleen M. Carley, "Estimating the Shape of Covert Networks," in *Proceedings of the 8th International Command and Control Research and Technology Symposium* (Conference held at the National Defense War College, Washington D.C., 2003).
[20] Kathleen Carley, "Estimating Vulnerabilities in Large Covert Networks," in *Proceedings of the 2004 International Symposium on Command and Control Research and Technology* (San Diego, CA, 2004).
[21] Carley, et al., "BioWar."
[22] Jana Diesner and Kathleen Carley, "Using Network Text Analysis to Detect the Organizational Structure of Covert Networks," in *Proceedings of the North American Association for Computational Social and Organizational Science (NAACSOS) Conference* (Pittsburgh, PA, 2004); R. Popping, *Computer-assisted Text Analysis* (London, Thousand Oaks: Sage Publications, 2000).
[23] Maksim Tsvetovat and Kathleen Carley, "On Effectiveness of Wiretap Programs in Mapping Social Networks," Workshop on Link Analysis, Counterterrorism, and Security, SIAM International Data Mining Conference (2006).
[23]Abbasi and Chen, 'Identification and Comparison"; Abbasi and Chen, *Applying Authorship Analysis to Extremist-Group Web Forum Messages* (IEEE Computer Society, September/October 2005): 67-75; Y. Zhou, et al., "U.S. Domestic Extremist Groups."

[25] Tami Carpenter, George Karakostas, and David Shallcross, "Practical Issues and Algorithms for Analyzing Terrorist Networks" (Telcordia Technologies, 2002).

[26] For history and political trends, see Ovid Demaris, *Brothers in Blood: The International Terrorist Network* (New York: Charles Scribner's Sons, 1977); Claire Sterling, *The Terror Network* (New York: Berkley Books, 1981); and Bruce Hoffman, *Inside Terrorism* (Boston: Little, Brown, and Co., 1987). Hoffman also addresses why people join terrorist groups. For psychology or terrorist attack tactics, including suicide, see Walter Reich, ed., *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind* (Woodrow Wilson Center Press: 1998); B. Bongar, L.M. Brown, L.E. Beutler, J. Breckenridge, and P. Zimbardo, eds., *Psychology of Terrorism* (New York: Oxford University Press, 2006); and Robert Pape, *Dying to Win: The Strategic Logic of Suicide Terrorism* (New York: Random House, 2005).

[27] Karl M. Van Meter, "Terrorists/Liberators: Researching and Dealing with adversary social networks," *Connections* 24, no. 3 (2001): 66-78.

[28] Ibid.

[29] Christopher Bellavita and Ellen Gordon, "Changing Homeland Security: Teaching the Core," *Homeland Security Affairs* 2, no. 1 (2006): article 1.

[30] Christopher Bellavita, "What is Preventing Homeland Security?" *Homeland Security Affairs* 1, no. 1 (2005): article 3.